Pipeline Leak Detection—Program Management

API RECOMMENDED PRACTICE

1175 SECOND EDITION, XXXX 20XX

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Users of this Recommended Practice should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

Foreword

Contents

Introduction

Background

The public, Congress, the National Transportation Safety Board (NTSB), and the Pipeline and Hazardous Materials Safety Administration (PHMSA) have a high level of interest in the subject of pipeline leak detection. PHMSA has been exploring issues involving leak detection program (LDP) effectiveness for several years, including through proposed rulemaking. Recent Congressional mandates and National Transportation Safety Board (NTSB) recommendations are attempts to address gaps in LDPs. The Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011 required the Secretary of Transportation to analyze technical, operational, and economic feasibility aspects on LDPs used by operators of hazardous liquid pipeline facilities and transportation-related flow lines. The Act also required a report to Congress and the issuance of rulemaking, if practical to do so. Along with this Recommended Practice (RP), PHMSA is working to address a leak detection related recommendation for natural gas transmission and distribution pipelines, as prompted by the NTSB. PHMSA has taken a number of initiatives to help address the congressional mandate and NTSB recommendation including sponsoring a public workshop on improving the effectiveness of LDPs in 2012, coordinating research and development forums and related solicitations in 2012 and 2014, and commissioning an independent study on leak detection in 2012.

PHMSA has communicated with industry on potential measures to further address leak detection effectiveness through related standards and asked the American Petroleum Institute (API) and the Association of Oil Pipelines (AOPL) for comment on whether expanding the existing API 1130, *Computational Pipeline Monitoring for Liquids,* or creating a new guidance document are viable options for addressing concerns of congressional mandates. In a joint response to PHMSA, API and AOPL chose the latter as the best approach to improve safety and made a commitment to develop this new RP for Pipeline LDP Management.

This pipeline LDP management Recommended Practice (RP) provides guidance to operators of hazardous liquid pipeline systems regarding a risk-based pipeline LDP management process.

This RP is specifically designed to provide operators with a description of industry practices in risk-based pipeline LDP management and to provide the framework to develop sound program management practices within an operator’s individual companies.

It is recognized that this RP creates requirements and practices that may take time to fully implement.

Objectives

This RP is written to provide guidance to operators for developing and maintaining management of pipeline LDPs. The elements of this RP are written to conform to current pipeline regulations and to encourage operators to “go beyond” and, in so doing, to promote the advancement or stronger utilization of LDPs in hazardous liquid pipelines.

This RP is intended to be used in conjunction with other industry-specified documents.

This RP builds on and augments existing requirements and is not intended to duplicate requirements of any other consensus standards or regulations.

While API 1175 is based on industry best practices, each operator is expected to tailor their LDP to their requirements.

The goal of an operator is to operate their pipelines safely and reliably so that there are no adverse effects on the public, employees, the environment, or the pipeline assets. This pipeline LDP management RP aids in this primary goal by the following.

— Providing hazardous liquid operators with guidance on development, implementation, and management of a sustainable LDP to minimize the size and consequences of leak events.

— Providing operators with enhanced guidance on selection of leak detection systems (LDSs) using a risk- based approach and on establishing performance measures for the capabilities of LDSs unique to each pipeline to meet or exceed the requirements of 49 *CFR* Part 195, such as in 195.452(i)(3), pertaining to leak detection related preventive and mitigative measures an operator shall take to protect a sensitive area.

— Addressing identified gaps and incorporating guidance into a comprehensive program document.

The LDP decisions rely on a thorough assessment and analysis of risk and threats as they apply to leak detection and should integrate with the operator's acceptable risk level. An LDP may reduce the consequence of a leak and contribute to the development from a "thinking to knowing" leak detection culture.

This RP does not include the following:

— detailed technical design of LDSs (as this is operator, LDSs, and infrastructure dependent);

— SCADA system design (as this is already covered in other API documents, for example API 1113, API 1164, API 1165, or API 1167);

— specific performance metrics (an individual operator's risk-based approach and engineering evaluation covers this);

— field response (as this is covered in an operator's emergency response plan);

— presentation of information to Controllers (covered in API 1165);

— equipment selection criteria (as these are specific to a operator, LDS, and vendor selection);

— a universal metric for pipeline leak detection performance (it is not a practical objective); or

— a definition of the relationship between emergency flow restriction devices (EFRDs) and leak detection (EFRDs and leak detection are two different mitigation systems).

Pipeline Leak Detection—Program Management

1 Scope

API Recommended Practice (RP) 1175 establishes a framework for Leak Detection Program (LDP) management for hazardous liquid pipelines that are jurisdictional to the U.S. Department of Transportation. This RP is an industry consensus document revised by hazardous liquid pipeline operators, leak detection manufacturers, consultants, and others. API 1175 focuses on using a risk-based approach to each operator's LDP. Reviewing the main body of this document and following the guidance set forth assists in creating an inherently risk mitigating LDP management system. API 1175 represents industry best practices in managing an LDP.

All forms of leak detection used by a pipeline operator should be managed in a coordinated manner. The goal of the LDP is to detect leaks quickly and with certainty, thus facilitating quicker shutdown and therefore minimizing negative consequences. This RP focuses on management of LDPs, not the design of leak detection systems (LDSs), and therefore contains relatively little technical detail. As with API RP 1130, API 1175 is intended for single-phase pipelines only; however, the approach may be applicable to pipelines that are not single phase.

Leak detection reduces the consequences of a LOC but does not reduce the likelihood of a leak. An appreciation and evaluation of leak event likelihoods, threats, and vulnerabilities drives the design of the LDP.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies (including any addenda/errata).

API Recommended Practice 1130, *Computational Pipeline Monitoring for Liquid*

API Technical Report 1149, *Pipeline Variable Uncertainties and Their Effects on Leak Detection Sensitivity*

API Recommended Practice 1160, *Managing System Integrity for Hazardous Liquid Pipelines*

API Recommended Practice 1167, *Pipeline SCADA Alarm Management*

US DOT 49 CFR Part 195

3 Terms, Definitions, Acronyms, and Abbreviations

3.1 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
continuous leak detection
Leak detection system that is operating in real time or near real time.

3.1.2
consequence level
Ranking of the possible consequences of a leak based on a calculated value or a relative value of the consequences.

3.1.3
dynamic leak volume

Amount of hazardous liquid that is leaked after the onset of a leak prior to the shutdown of the pipeline or other appropriate operational response is initiated.

NOTE This is also known as pumped volume.

3.1.4
escalation barrier
Functional group of safeguards, such as primary containment processes, equipment, engineered systems, operational procedures, management system elements, or worker capabilities designed to prevent loss of containment (LOC) and other types of asset integrity or process safety events and mitigate any potential consequences of such events.

3.1.5
externally based leak detection systems
leak detectors
Applications that use sensors to directly detect the presence of a hydrocarbon or physical changes in environment due to a leak.

NOTE These sensors are placed on or near the external surface of the pipe or, in the case of cameras for instance, within sensing range of the pipeline.

3.1.6
groupthink
Psychological phenomenon that occurs within a group of people in which the desire for harmony or conformity in the group results in an irrational or dysfunctional decision-making outcome.

NOTE NTSB has several publications related to this phenomenon under the topic Crew Resource Management.

3.1.7
independent means
That which may be a separate or complementary leak detection system that uses another technique, some verification method, separate calculations, leak detection specialists' involvement, or other procedure or process.

3.1.8
internally based leak detection systems
Applications that are internally based using field sensor data that monitor internal (and perhaps related external) pipeline parameters but are not actually detecting the presence of hydrocarbons.

NOTE Since these systems do not actually contact leaked hazardous liquid, internally based leak detection systems may be regarded as inferential systems (see API 1130).

3.1.9
leak detection

a) leak detection method

Classification of leak detection operation as being continuous or non-continuous.

b) leak detection principle

Classification of leak detection by categories that are externally based or internally based.

c) Leak Detection Program (LDP)

Top-level term that encompasses all the various LDSs (which may include multiple techniques) employed by the operator and identifies all methods used to detect leaks and the policies, processes, and the human element.

d) leak detection technique

Individual technology applications (e.g. real time transient model, wetted cable, fiber optical cable, etc.) used to detect or indicate a leak.

e) Leak Detection System (LDS)

End-to-end application of one technique that may be internally based or externally based and continuous or non- continuous.

f) complementary LDS

LDS that uses a different technique, has different metrics, and may be independent of the inputs for the primary technique.

3.1.10
leak indication
Alarm or other notifying event that suggests that present conditions indicate the possibility of a leak.

NOTE 1 The possibility of a leak is stronger if there is more than one indication.

NOTE 2 Industry also uses the word “triggers” for leak indications.

3.1.11
leak monitoring
Form of pipeline leak detection that is intended to detect the occurrence of a leak smaller than a rupture.

3.1.12
leak verification
Analysis of pipeline operation and/or pipeline conditions triggered by the suspicion of the existence of a leak intended to provide sufficient confidence to make a formal determination of whether or not a leak exists.

NOTE It may involve onsite investigation.

3.1.13
loss of containment
LOC
Unplanned or uncontrolled release of hazardous liquid to the environment.

NOTE 1 The words leak, spill, release, fluid release, or commodity release are sometimes used for a LOC.

NOTE 2 Sometimes this is called loss of primary containment or LOPC.

3.1.14
metrics
performance metrics
Performance category that is quantified by Key Performance Indicators (KPIs).

NOTE Leak detection metrics are described in API 1130, Annex C and are grouped into four categories, or metrics, that determine a system's reliability, sensitivity, accuracy, and robustness.

3.1.15
non-continuous monitoring
Type of leak detection that is periodic but not in real time.

3.1.16
overall leak volume
Total leak volume that occurs from the time the pipeline leak begins until all leakage is stopped.

NOTE It includes dynamic leak volume plus static leak volume.

3.1.17
risk tolerance
acceptable risk
Amount of risk that the operator is willing to assume.

NOTE When the level of risk is above an acceptable level or is not tolerable it exceeds the risk tolerance.

3.1.18
risk-based approach
Decision-making process that prioritizes the leak detection work based on the calculated risk, evaluates it against a level of risk tolerance, and then takes action to reduce the risk to a tolerable level.

3.1.19
rupture monitoring
Form of pipeline leak detection that is intended to swiftly detect the occurrence of a rupture.

NOTE What constitutes a rupture is determined on a pipeline-by-pipeline basis and is defined by an operator.

3.1.20
sensitive area
Specific locales and areas, not limited to HCAs or USAs, in or by the pipeline ROW where a leak may have significant adverse consequences to any or all nearby people, the environment, and community assets.

NOTE See 49 *CFR* Part 195 for definition and description of HCAs and USAs

3.1.21
static leak volume
Amount of hazardous liquid that is leaked after the shutdown of the pipeline (or other appropriate operational response if applicable) is initiated.

NOTE This is known as drain-down volume.

3.1.22
tuning
Process where the function of the leak detection technique is adjusted for more precise functioning.

3.2 Acronyms and Abbreviations

For the purpose of this standard, the following abbreviated terms apply.

CMMS	computerized maintenance management system
CPM	computational pipeline monitoring
CRM	control room management
DOT	Department of Transportation
FAQ	frequently asked question
FMEA	Failure Mode Effects Analysis
HCA	high-consequence area
IMP	integrity management program
KPI	key performance indicator
LDP	leak detection program
LDS	leak detection system
LOC	loss of containment
MMS	maintenance management system
MOC	management of change
OJT	on-the-job training
PHMSA	US DOT Pipeline and Hazardous Materials Safety Administration
PPTS	Pipeline Performance Tracking System

RACI Responsible, Accountable, Consulted, Informed

RAM Reliability, Availability, and Maintainability

RCM Reliability-Centered Maintenance

ROW Right of Way

RP recommended practice

SME subject matter expert

4 Leak Detection Program

This document should be viewed as a listing of best practices to be employed when planning, selecting, designing, analyzing, implementing, maintaining, and empowering a culture within a Company's pipeline Leak Detection Program (LDP) management. While this document addresses hazardous liquid pipelines regulated under *CFR* 49 Part 195, the philosophy may be applied to non-regulated pipelines as well. In adopting the recommendations of API RP 1175, operators should progressively implement changes and establish a timeline for the associated work. Pipeline leak detection should be managed by structuring the various elements of leak detection into an LDP. An LDP should promote a strong leak detection culture, which is critical in managing the human component of an LDP. This document outlines the following components of an LDP:

- management commitment and leadership;
- stake holder engagement;
- employing risk management and technique selection criteria;
- operational controls;
- incident investigation, evaluation, and lessons learned;
- continuous improvement to the LDP;
- emergency preparedness & response;
- competence awareness & training;
- documentation and record keeping.

4.1.1 Details of the Essential Elements of the Leak Detection Program

Expanding on the strategy elements:

a) Management commitment and leadership. A written strategy document should clearly show management is engaged and has a commitment to a comprehensive LDP. The leak detection strategy document should cover roles and responsibilities of all employees and stakeholders who are involved with the operator's LDP. Management should demonstrate its commitment through resources allocation, visibility, and leadership as outlined in the strategy. For the LDP, management should promote engagement and leadership at all levels of the organization. There should be a commitment to creating a culture that moves from "thinking leak mitigation" to "knowing what is in their leak mitigation strategy." Management should review and endorse an annual report on the LDP.

   This is discussed in detail in 5.

b) Operator's requirements and goals. Overall or broad goals for the LDP should be established and endorsed by management. The operator should require that dependent and interrelated functions within the organization are sharing information and working as a team to achieve the goals. The operator should ensure there is a clear connection between goals and day-to-day work activities. Management may set targets for performance aspects of the LDP. The strategy may set limits for non-leak alarms so the confidence in the LDS is not eroded by too many alarms. The strategy may specify a worst-case leak from a corporate point of view that may not be a rupture or large leak volume, or a target may specify an improvement in the leak detection performance metrics (for examples: an annual reduction in detection alarm thresholds by x % or improvement in localization, accuracy, and/or time to detect). The strategy may note what the operator wants to achieve in the future.

c) How requirements and goals may be satisfied. The selection of LDSs chosen for the LDP shall cover all regulatory requirements and should cover operator requirements and goals. The LDSs should be implemented and maintained so the users have confidence in leak alarms. The strategy should always emphasize the adherence to approved procedures and processes. The operator should utilize the overall operating experience of their pipelines, and of their individual pipelines to maximize the capability of the LDP. In some cases, the strategy may outline types of equipment that may be used with the LDSs (e.g. types of meters). The LDP strategy should include continued awareness of developing technologies and the output of industry led initiatives to validate new technologies and approaches.

d) Employing risk management. The framework of the LDP shall be based on a detailed risk assessment. The assessment should cover the leak detection required performance and reduction in risk level provided by an LDP. The LDP may work with the integrity management program (IMP) to ensure factors related to leak detection are in the risk assessments for each pipeline. All aspects of the LDP (e.g. selection of LDSs) may be dependent on the acceptable risk that the operator is willing to assume. Risk assessment may be used to change the level of application of the LDSs based on short term increased risks. A primary criterion within an operator's risk management program is LDP performance. Also to be evaluated are mitigating factors such as the operational response and emergency response in the event of a leak along the pipeline.

e) Selection of LDSs. The leak detection strategy document should cover all aspects of pipeline operations that affect the LDSs and the principles, methods, and techniques that are or will be used. The selection may focus on proven and industry common LDSs. Some aspects of leak detection are prescribed in regulations (i.e. visual surveillance and landowner awareness); however, the detailed application of these LDSs should be determined by each operator. The leak detection strategy document should address leak detection requirements during design of new or changes to existing pipelines. The selection should outline why particular LDSs are chosen. The operator may implement multiple LDSs that complement one another. The focus of selection should be on methods that provide continuous leak detection. Selection should cover issues such as increased risk in some areas, utilizing industry best practices, employing LDSs that may be tested and may have well defined KPIs or because no other LDS is possible. Selection should establish performance expectations that may be used for benchmarks for ongoing testing.

f) Integration of all forms of leak detection employed. Whenever possible, the outputs of all LDSs that are employed should be integrated. This suggests that all LDSs should be coordinated so they all support the goal of detecting leaks on the pipeline.

g) Regulatory requirements and industry standards. The strategy should list or refer to a list of all regulatory references and any industry standards that apply to the LDP. The strategy document should outline how these regulatory and industry standards are applied and perhaps which parts do not apply and why.

h) Ongoing measurement of performance of the LDP. The individual LDSs shall be tested or evaluated on a periodic basis or when there is a need to do so. The strategy should state that the overall LDP performance shall be evaluated annually, not to exceed 18 months. The overall evaluation may include comparison to performance achieved by other operators. The LDS document should emphasize the importance of having methods to measure performance (sensitivity, reliability, accuracy, robustness) using measurable KPIs. The health of the leak detection culture should be assessed or tested. The evaluation may be by comparison to industry best practices.

i) Reporting. Reports to levels of management may be on a periodic basis but there should be a periodic report on the LDP to management, not to exceed 18 months. Changes based on these reports should be passed to an improvement process.

j) Training, testing, and operations/procedures. The strategy should make a commitment to rigorous training of employees and appropriate level of training for other stakeholders. A training program should be developed to not only train employees and stakeholder in the technical aspects of their work, but also their roles and responsibilities as a part of the leak detection team. The strategy should outline a requirement for testing of the LDSs or evaluation of LDSs to ensure that design performance is maintained. The strategy shall outline the requirements for procedures and the application of procedures during operation.

k) Review and approvals. The operator should periodically review their LDS document to ensure it is up-to-date. The LDS should be modified as needed and reaffirmed with management of the operator.

l) Management of change. The strategy shall outline the requirements for management of change because operation of the LDP involves many functional areas of pipeline operation. Subtle operational or equipment changes may have an adverse direct impact on leak detection unless they are tightly controlled and managed.

m) Ongoing improvement of the LDP. Continual improvement requirements in the LDP should be outlined in the strategy. The LDS should indicate the importance of and support for an improvement process to address gaps if the targets are not met and to accommodate changes to regulations, pipeline operations, assets, stakeholder expectations, and overall improvement of the LDP. The operator may indicate a goal of improvement by, for example, evaluating industry best practices and lessons learned. Improvements should help move toward training improvement and strengthening of the culture. The strategy may indicate the desire to evaluate new technologies and the output of industry led initiatives to validate new technologies or be involved in leak detection R&D to improve the leak detection capabilities.

Figure 1 provides a flow chart outline of the LDP management process. It shows all the aspects of LDP management that are outlined in API RP 1175 and the relationship of the various aspects. This figure represents the process for most operators, but it is not intended that the aspects shown are followed explicitly.

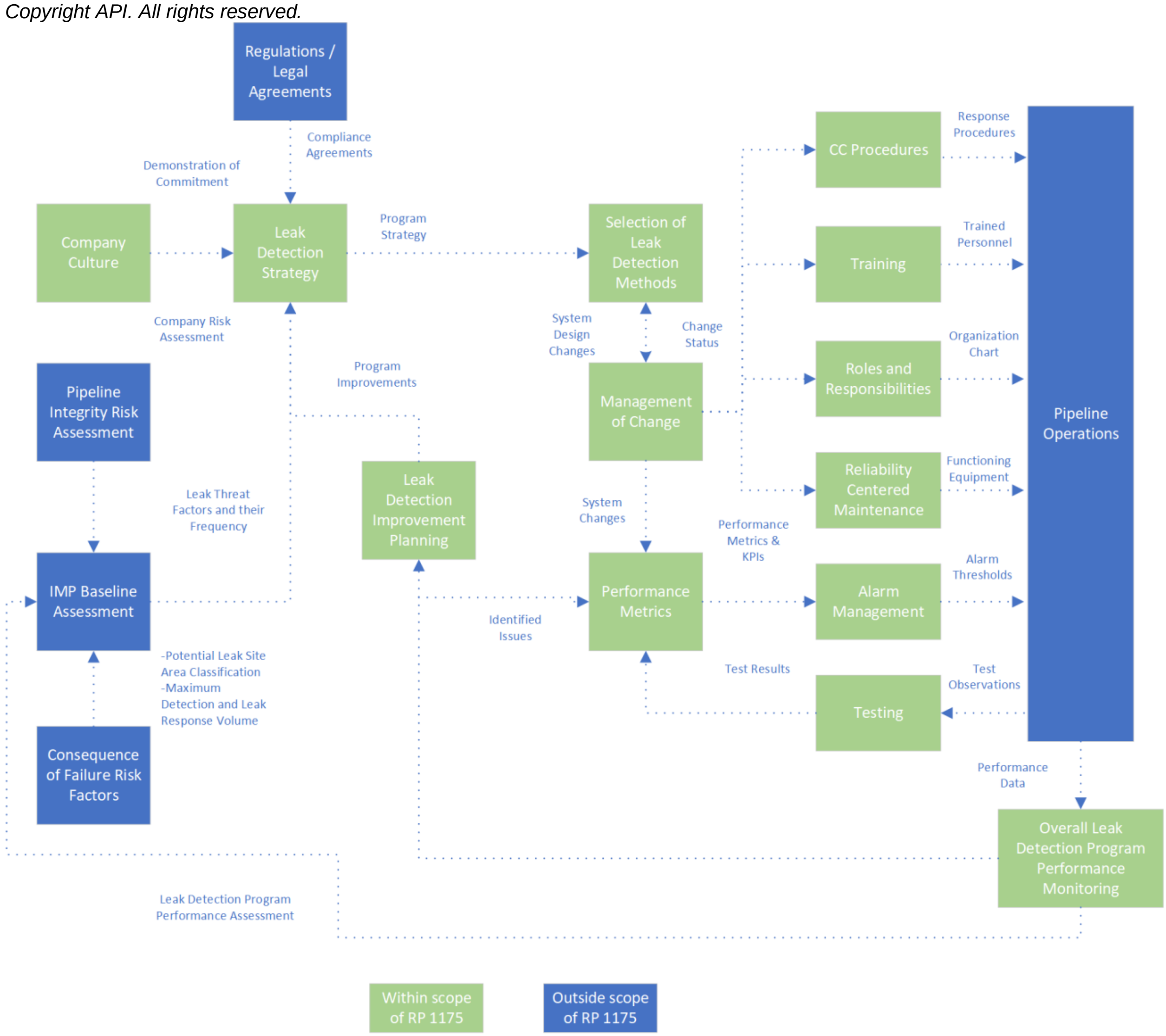


Figure 1—Leak Detection Program Flow Diagram

The operator shall develop and implement a leak detection program. The LDP shall be documented, and that documentation should cover all aspects of the LDP, define the goals of the LDP, and outline how the LDP will meet those goals.

5 Management Commitment and Leadership

5.1 General

Top management shall establish goals and objectives for an operator's leak detection program. The objectives shall be measurable and consistent with overall leak detection policies.. Top management shall also create a culture within the organization that encourages openness and two-way dialogue so learnings from incidents and events can ultimately reduce the risk of recurrence. The health of this culture should be assessed, and leadership commitment needs to be visible to address areas of concern and opportunity.

5.1.1 Responsibilities of Leadership

Operators should comply with Sections 5.4, 5.5, and 5.6 of API RP 1173 with regards to leak detection.

5.2 Leak Detection Culture

Operators should develop a strong leak detection culture. An LDP includes not only the technology, but the people involved in applying the technology. Improving an organization's culture moves its people from thinking about safety and integrity to practicing safety and integrity.

Leak detection culture is visible by the level of commitment of all employees, particularly an organization's management.

Leak detection is an integrating discipline that relies on major functions of an organization working together to be successful. A strong leak detection culture that promotes prompt and appropriate actions throughout the organization's hierarchy is essential to the success of a leak detection program.

5.2.1 Culture Indicators

The following behaviors are indicative of a strong leak detection culture:

— Ongoing support towards continuously improving pipeline leak detection, even if the operator is meeting current leak detection goals.

— Coordination and collaboration between the different entities involved in the LDP.

— Ongoing training of relevant staff regarding how each person supports the leak detection program.

NOTE API 1168 describes control room management practices, including training for Controllers

— A focus on safe and reliable operation of the pipeline with no negative repercussions on the staff who take actions in response to leak indications. This includes:

  — Shutdown when there is a leak indication. When in doubt, shut down and then assess;

  — Policies and training on Stop-Work-Authority (SWA) or Stop-Work-Responsibility (SWR).

6 Stakeholder Engagement

6.1 General

Stakeholder engagement plans should be developed using the guidance in API RP 1173.

Stakeholder engagement plans should include information on leak detection and its relevance to particular stakeholder audiences.

7 Risk Assessment

7.1 General

The framework of the LDP should be based on a detailed risk assessment.

The risk assessment should identify the LDSs required in an LDP.

An example of a risk assessment is included in Annex A.

7.2 Risk Assessment Factors

The risk assessment should be developed with consideration of the pipeline's integrity management program (IMP) to ensure that factors included in the IMP are built into the leak detection risk assessment. All aspects of the LDP, including selection of LDSs, is dependent on the acceptable risk that the operator is willing to assume.

Refer to API RP 1160 for further information on integrity risk assessments.

The risk assessment should evaluate the existing operational LDP elements as they relate to mitigating the consequences of a leak. Integrity management activities should be evaluated along with the pipeline segment's characteristics to determine the likelihood and consequence of a failure occurring. The risks associated with LOC differ for various pipelines, hazardous liquids being transported, and their location. A specific risk analysis and evaluation may be performed for LDSs on each individual pipeline system or segment; typically called a leak detection capability evaluation.

7.2.1 LOC Risk Factors

Elements for inclusion in the risk assessment pertaining to the probability and consequence of an LOC include:

- Review of the IMP, particularly the integrity risk assessment results:
    - IMP risk reduction initiatives.
- Review of the existing pipeline infrastructure, possibly including:
    - age of pipe,
    - history of pipe,
    - operating pressure-to-hydro test ratio (i.e. the safety margin),
    - diameter,
    - length,
    - size,
    - type of hazardous liquid carried,
    - pipeline profile,
    - high-consequence areas,
    - ignition sources,
    - specific terrain between the pipeline and the high-consequence area.
- Review of known leaks and their causes,
- Isolation capability (pumps, number of valves, and the types and their locations). Note that the current regulations already require a risk assessment as part of the normal pipeline integrity management process that incorporates evaluation of valve operations with leak detection performance.
- Emergency response/leak response capability, including nearest locations of response personnel and time to respond.
- Environmental factors.
- Other considerations.

Risk assessments may be used to change the application and tolerances of LDSs based on short term increased risks, which can include, for example, nearby construction, natural hazards, or operational changes. The risk assessment should evaluate mitigating factors such as the operational response and emergency response in the event of a leak along the pipeline.

A risk-based approach should be applied to the evaluation of an operator's LDP and should list factors fundamental to the selection process. Since the risk-based approach should evaluate overall risk, consequences, and likelihoods, the operator may look at all three of these items during the selection process.

7.2.2 Factors Affecting Risk Mitigation

Some mitigation factors are within the scope of a leak detection program and should be included in the risk assessment. These factors can include:

— Leak detection capability of the existing LDSs:
  - performance metrics: reliability, sensitivity, robustness, and accuracy;
  - KPIs and evaluations of the LDSs;
  - primary, complementary, alternative LDSs in place and their coverage.

— Leak detection capability of the existing LDP:
  - strength of the leak detection culture;
  - strength and completeness of the strategy.

7.3 Risk Tolerance

Figure 2 shows how an overall risk score for various pipelines or pipe segments may influence the selection and application of LDSs within operator's leak detection strategy. Each vertical bar represents the cumulative risk score for a pipeline or pipeline segments.

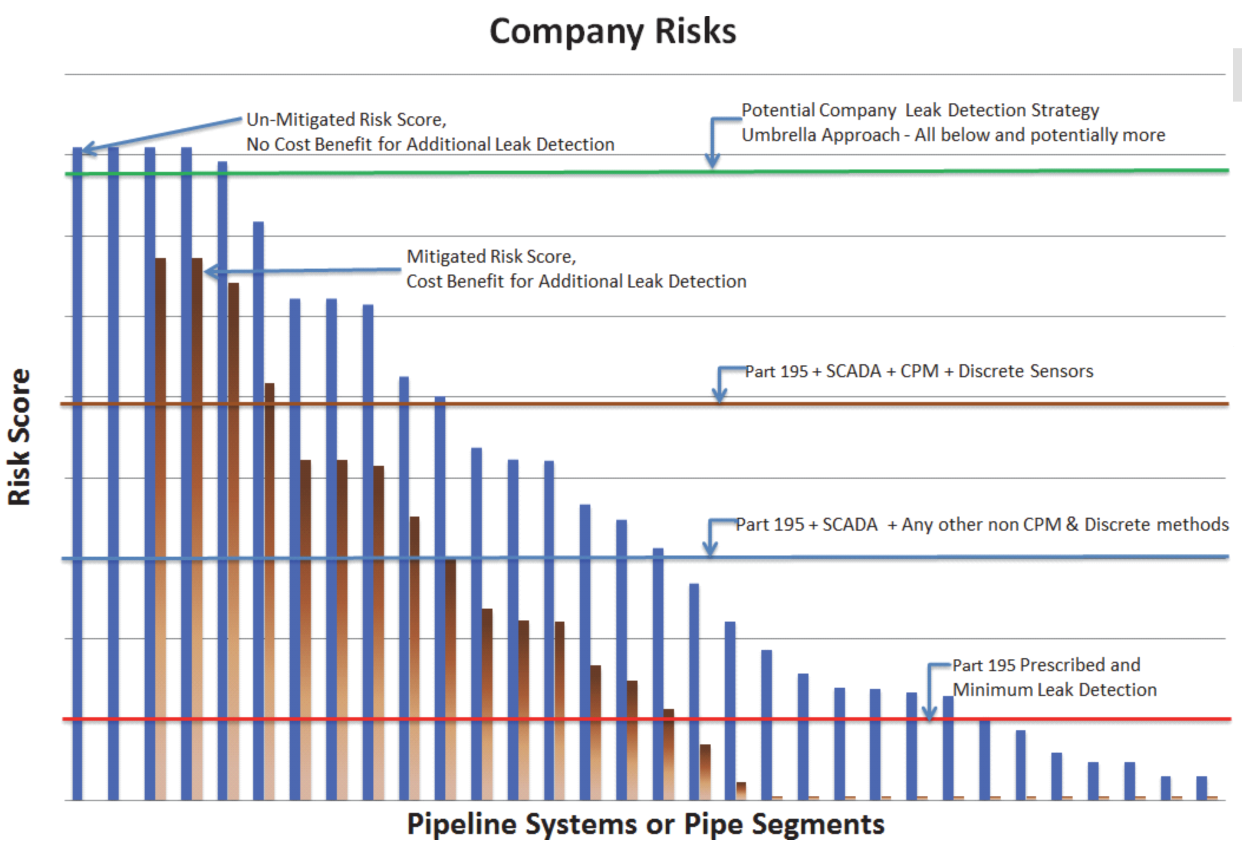


Figure 2—Risk Assessment

A high-risk score equates to a higher consequence and/or higher likelihood of failure. This implies that pipelines that have a high-risk score should have a leak detection strategy that goes above and beyond regulatory requirements.

The horizontal lines represent the operator's decision on what type of leak detection strategy is appropriate at a given risk level. The LDP that meets operator requirements that are outlined in the operator's strategy are shown above the level of the minimum required leak detection line in the figure. For example, the horizontal lines exceed the risk level, and the leak detection strategy represents a tolerable risk.

If a pipeline's mitigated risk exceeds the level of the highest horizontal line, then changes may be made to the pipeline's operation, its physical characteristics, or the leak detection strategy. Examples of the types of changes can include: changing the hydraulics; changing the MOP; segmenting the line with additional integrity meters; or the addition of a more appropriate leak detection method in the LDP. In some cases, the operator may specify the acceptable length of time to operate above the highest horizontal line.

Selection of leak detection strategy for each pipeline or pipeline segment should consider the practicality of implementing the strategy in relation to the risk mitigation benefit.

8 Selection of Leak Detection Methods

8.1 Selection Process Overview

LDSs are implemented to provide early notification of loss of containment (LOC), so action may be taken to mitigate the consequence of the leak. An LDS is intended to decrease the spill volume by shortening the time required to detect a leak within its detectable range and assisting in identifying the leak location. Once a leak is detected, an operator can initiate a shutdown take actions to manage the leak.

The intent of this section is to help operators select which LDSs and associated leak detection principles, methods, and techniques to include in their LDP. This selection process may be used for the selection of new applications, to add additional LDSs, or to re-examine existing LDSs.

The selection of LDSs, leak detection principles, methods, and techniques are a multifaceted, multi-step, iterative process that may include the following elements:

— performing an risk assessment;

— considering the LDS selection to cover particular constraints of individual pipelines and individual threats;

— evaluating gaps in the LDS for operating modes;

— incorporating regulatory requirements;

— evaluating industry knowledge;

— integrating the operator's requirements;

— aligning the selection with the operator's leak detection culture and strategy;

— evaluating the available technology for leak detection;

— linking the operator's performance metrics, KPIs, and targets;

— considering primary, complementary, and perhaps alternative LDSs.

If an LDP is already in place, this selection process may be applied to validate the selection. The selection process should be documented.

8.2 Risk Assessment

Risk assessment is a critical part of the LDS selection procedure. The risk may be compared against the operator's risk tolerance.

See 7 for further description of a leak detection risk assessment.

8.3 Incorporating Regulatory Requirements

In the US, the primary regulatory requirements for liquids pipelines are outlined in 49 *CFR* Part 195.

In Canada, the primary regulatory requirements for liquids pipelines are outlined in CSA Z662.

8.4 Evaluating Industry Knowledge

There are several related RPs, standards, and publications related to leak detection. Those necessary to implement this RP are noted in 2. Sources of additional information that may be useful are listed in the Bibliography. Additional research in leak detection is ongoing and continual improvements to an LDP should incorporate improved technologies and methodologies.

8.5 Integrating Operator Requirements

In addition to ensuring LDSs satisfy all regulatory requirements, an Operator should identify LDSs which meets their own internal requirements. While it is typical for larger operators to have additional internal requirements, it is not intended to imply that every operator needs to have their own set of requirements. The decision whether to evaluate LDSs against operator requirements resides solely with each operator and should be a needs-based decision driven by the results of their risk assessment. These requirements, where applicable, can be as highly specific or general as an operator chooses and can be based on functionality (i.e. the presence of a user interface or leak location capability), methodology (i.e. using a specific detection technique), historical experience (i.e. a system or technique an operator is familiar with), or some other criterion the operator deems vital to their selection process. Due to the list of potential requirements being as varied as the principles, methods, and techniques available, this section cannot provide an all-encompassing list nor can it recommend elevating one requirement over another.

8.6 Leak Detection Strategy Requirements

The leak detection strategy may be satisfied in part by selection of leak detection systems (LDSs) that best fit the requirements of the strategy. The strategy may for example set several goals and targets. These should be understood and accommodated during the process of selecting LDSs. For example, the strategy may require primary and complementary LDSs.

The leak detection design and selection aspects should be aligned with the operator's KPIs (which are discussed in 15). The overall goal of a pipeline leak detection strategy is to provide the resources required to positively identify an LOC from a hazardous liquid pipeline within a time period that is commensurate with the associated level of risk. These resources should encompass the technology, processes, and trained personnel to monitor the pipelines to ensure indications supporting a possible LOC are rapidly acknowledged and acted on.

To meet the requirements of the strategy, the operator may implement complementary and alternative LDSs as a part of the LDP. The main LDS may be called the primary LDS by the operator. However, the designation "primary LDS" is not simply defined. An LDS that is primary during operation may not be primary on a shut-in pipeline when another LDS may be more reliable. Most often, a continuous method is chosen as a primary. On many pipelines, a CPM technique is commonly the primary; however, an externally based LDS may satisfy the leak detection strategy.

A complementary LDS may be designated as such. It may be continuous. A complementary LDS may use a different technique, have different metrics, and may be independent of the inputs for the primary technique. In some cases, depending on risk, more than one complementary LDS may be implemented throughout the pipeline system or just in specific segments if it is not practical to implement across the entire pipeline system.

An alternative LDS may be chosen that may be used if the primary LDS is out of service. Usually, an alternative LDS is used under closely supervised leak detection monitoring of the pipeline operation.

There may be other LDSs that are designated as redundant (i.e. have the same function as another LDS and exist so that LDP does not fail if the primary or complementary LDS fails). The redundant LDS may be running and mirroring the system to which it is redundant so fail-over is automatic; or there may be a backup LDS used to replace an LDS that fails. The backup may be made active when it is required.

Table 1 is a visual example of an LDP that shows leak size classifications, the LDS that may be used for leak detection, and an unspecific factor of time to detect LOC. Information on the definition of the various leak sizes is found in API 1130, Annex B.

Table 1 – Visualization of an Example LDP

	Leak Type	SCADA Monitoring	CPM	Public Awareness	Aerial Surveillance	In-line Inspection
Leak Rate ↑	**Rupture**	√	√	√	√	N/A
	Medium Leak	○	√	√	√	√
	Small Leak	X	○	○	√	√
	Seep	X	X	○	○	√
	Time-to-Detect →					

√ Detection Probable

○ Detection Possible

X Detection Improbable

8.7 List and Classification of LDSs

The LDSs that may be used to detect leaks cover a wide spectrum of techniques, principles, and methods. The techniques vary from surveillance to hydrocarbon sensors to real-time monitoring software. The principles employed may be externally or internally based. The methods may be continuous or non-continuous. Table 2 provides an example list of the leak detection techniques and categorizes them as to whether they are internally based or externally based and continuous or non-continuous. Table 2 is not intended to be a comprehensive list of leak detection techniques.

Each practical LDS has its strengths and weaknesses that are dependent on the characteristics of the LDS, the specific application, the leak detection technique, its maturity, and the complexity of the pipeline to which the LDS is applied. In combination with processes or procedures, applying the appropriately selected LDSs is the key to effective pipeline LDP.

It is important to note the following when investigating the various techniques for leak detection.

— additional instrumentation may need to be added to the pipeline to support a particular technique.

— additional maintenance, support, and testing may be required for some techniques.

— some existing techniques may be enhanced. For example, the visual aspect of surveillance may be enhanced by the addition of infrared sensors.

Not all the techniques listed in Table 2 are proven; some are still being evaluated for practicability in industry. Practical techniques are readily available, potentially operator deployed, and possess some form of adequate field-based installation. This list is not intended to be all inclusive; new techniques for leak detection are continuously under development by industry.

- non-Continuous, Externally based;
- non-Continuous, Internally based;
- continuous, Externally based;
- continuous, Internally based;

Table 2—Example LDS Techniques

	Externally Based		**Internally Based**	
	Physical Inspection	**Sensor-Based Monitoring**	**Manual Observations**	**Computational Pipeline Monitoring**
Non-Continuous	Aerial Surveillance	Ground-Penetrating Radar	Volume or Line Balance Calculations	
	Ground-Based Line Surveillance	Sniffer Tubes	Hydraulic Calculations	
	Hydro Testing	Tracer Chemicals	Pattern Recognition	
	Satellite	Intelligent Pigs	Shut-in Testing/Stand-up Testing	
	One Call System/ Public Awareness	Soil Sampling		
Continuous		Sensing Cables	Controller SCADA Monitoring	Conservation of Mass
		Acoustic Sensors		Pressure Monitoring
		Cameras		Line Balance
		Chemical Analyzers		Acoustic Negative Pressure Wave Monitoring

During LDS evaluation, it may be helpful to discuss the application and expected performance with the vendor and/or other users of the specific LDS. Each pipeline operation is unique, and the actual performance of the same LDS applied to two different pipelines may vary significantly.

8.8 Leak Detection Technology

Applications that use sensors (or leak detectors) to directly detect a commodity release are called externally based systems. Applications that indirectly detect or infer commodity releases are called internal based systems.

8.8.1 Externally Based Leak Detection Systems

Externally based pipeline leak detection systems (often called leak detectors) detect evidence of a commodity's presence outside of the pipeline or its exiting the pipeline. In these systems, the local detector may send an alarm signal to the Control Center for display and annunciation.

Common types of externally based systems or devices include:

— fiber optic leak detection cables.

— hydrocarbon sensing cables.

— acoustic emissions detectors.

— cameras.

— foot patrols.

— aerial inspection.

— hydrocarbon sensors (including those with vapor pick-up tubes).

8.8.2 Internally Based CPM Systems

CPM systems analyze real-time data to infer evidence of a leak and present that evidence and other calculated information for the Controller to evaluate and take appropriate action. The degree of complexity in processing field data varies from simple comparisons of a parameter relative to a threshold limit to more extensive analysis of multiple parameters that may include pattern recognition, machine learning, statistical analysis, and other techniques.

Common types of internally based CPM techniques include:

— line balance methods (Line Balance, Volume Balance, Modified Volume Balance, Compensated Mass Balance).

— real Time Transient Model.

— pressure/Flow Monitoring.

— acoustic/Negative Pressure Wave.

— statistical Analysis.

Refer to API 1130 for further discussion of CPM systems.

8.9 Evaluating and Selecting Suitable Technologies

After evaluation of risk, operator strategy, and regulatory requirements, the operator should develop a list of selection criteria and select LDSs. There are three key areas of inquiry: what features are needed, what performance is required, and the process of the selection criteria to evaluate a prospective LDS.

When selecting the LDS that is to be employed in the LDP, the operator should be cognizant of its range of applicability and any potential limitations inherent to the LDS that could impact its ability to accurately detect leaks in the field. The performance should be quantified by use of metrics and related KPIs.

There are several factors related to physical environment and hazardous liquids transported that may affect the leak detection method(s) selected. These include elevation profile, waterways (rivers, lakes, streams, oceans, etc.), major thoroughfares, spans and bridges, fluid properties, limitations of the location, meteorology, radiant heat effects, etc.

The selection may evaluate additional functionality that may be obtained from LDS systems, such as the using fiber optic cable to support telemetry for pipeline communications, public address and general alarm (PAGA) systems, closed-circuit television (CCTV), and private automatic branch exchange (PABX).

When designing an LDP, operators should maintain an overall system view and recognize that each component works with the others to provide the desired performance. Different components play different roles in mitigating the overall consequences of a release. Table 1 shows an example of different categories of LDSs defined by their relative time frame.

The choice of an LDS(s) may be impacted by pipeline characteristics such as:

— non-regulated pipelines;

— pipelines that do not or cannot have all the required instrumentation;

— pipelines that pose challenges for effective leak detection, such as those operating with two-phase or multiphase flow;

— pipelines with a history of small (seepage) leaks;

— pipelines with a history of ruptures;

— pipelines with unique operating histories that characterize significant operational challenges.

8.10 Modifying Selection for Particular Requirements of Individual Pipelines or pipeline segments

LDSs are engineered systems, meaning that the same LDS applied to multiple pipelines may have different results or the LDS may not perform as well on some pipelines. Perhaps an additional LDS or modification to the LDS may be needed to accommodate leak detection on other pipelines or pipeline segments; or perhaps installation of additional instrumentation or changes to operation may be required.

8.11 Periodic Review of Selection

The operator may periodically evaluate the selection of LDSs to ensure they are meeting the requirements of the leak detection strategy. Possible reasons for the review may be:

- population or environmental changes that may have occurred around the pipeline,
- when technology or operating conditions warrant, or
- the periodic review may be performed on a timed cycle.

One potential approach to a timed cycle is to review the leak detection requirements based on a five-year cycle, similar to a baseline IMP. The review would look at the items outlined in regulation and use a team of leak detection and risk experts who would utilize a risk matrix or other ranking process. In particular, the team may look at SAs, leak detection alarms, and any other performance-related information. The purpose is to keep the LDP current with this information. The selection process outlined may then be re-applied to the new conditions.

Improvements or other changes to LDSs or the LDP may be triggered by new circumstances such as:

— program modified by field experience;

— application updates;

— availability of new LDSs or extensions, to be evaluated by selection criteria;

— technology review cycle;

— IMP evaluation review;

— re-evaluation of the leak detection methods based on an established cycle;

— new pipelines have been built or acquired;

— pipeline service is changed or there are significant instrumentation or measurement changes;

— change of regulatory requirements;

— leak detection strategy change;

— a requirement for enhanced leak detection.

9 Performance Targets, Metrics, and KPIs

9.1 General

Hazardous liquid operators should establish performance targets for their LDSs and define and track KPIs to ensure the performance targets are met. Typically, these performance targets are set as part of the operator’s leak detection strategy, and the leak detection selection process attempts to select and implement the LDSs that will meet these targets.

In this RP, the terms “metric” and “KPI” are closely related. The metrics (e.g. reliability) are quantified by the KPIs (e.g. number of non-leak alarms) of the metric. KPIs and their targets should be specific and measurable quantities designed and implemented to facilitate the attainment of desirable overarching goals of an operator’s LDP. These metrics are defined as sensitivity, reliability, accuracy, and robustness which are described below. These KPIs are quantified by the operator. The leak detection vendor may assist as well.

Performance targets and KPIs may exist at the LDP level for a specific LDS and for a specific instance of the LDS, i.e. its implementation on a particular pipeline or pipeline segment. The operator's performance monitoring of an overall LDP is discussed in 15 of this RP and covers KPIs at the program level.

Determination of the leak detection KPIs and performance targets are predicated by the goals of the operator's leak detection strategy.

The KPIs and performance targets in turn influence the selection of LDSs, both in terms of which LDSs are available in the LDP and which LDS or LDP is applied to specific assets. The leak detection targets are refined by the LDP's continual improvement process and by performance monitoring. The leak detection metrics and associated KPIs are designed to verify that performance targets are being met and to provide diagnostic information if they are not. The KPIs should be analyzed statistically to deduce appropriate performance targets.

An option may be to use an independent third party to evaluate the LDS and management of KPIs.

9.2 Performance Metrics and Key Performance Indicators

9.2.1 Goal and Targets

Performance metrics and KPIs should be defined, computed, and tracked to establish that leak detection goals are being met. The corresponding performance targets are then refined and revised as part of the continual improvement process. KPIs should be designed to allow the operator to gauge the degree to which the goals are being met. The availability of KPIs should be evaluated when deciding on the leak detection goals. Goals that are overly broad or subjective are difficult to measure effectively. On the other hand, goals that are too specific or prescriptive may be more challenging to refine and revise, depending on the complexity of the pipeline system and the number of LDSs implemented. Such goals may limit an operator to a specific LDS vendor, etc., that may be difficult to upgrade or replace. Annex D provides an example of performance metrics and targets for a CPM and for an external LDS.

9.2.2 Performance Metrics

Selection of an LDS system for a given pipeline involves evaluation of the required and expected (or estimated) performance of the system. Other aspects such as commercial considerations (e.g. use of a common system in a Control Center with multiple pipelines) or economic criteria (e.g. capital and operating cost of the LDS) may be considered but these are not discussed herein.

The following categorizes and describes performance metrics for selection consideration. During the selection, the operator may place more weight or importance on one metric or another. A system should achieve a satisfactory balance between all four of these performance metrics. For a more complete description of these metrics please refer to Annex D.

— *Reliability*. The measure of the LDS' ability to render accurate decisions about the possible existence of a leak on the pipeline while operating within an envelope established by the LDS design. A system is considered more reliable if it consistently detects actual leaks without generating false alarms as defined by the operator's alarm management plan / program.

— *Sensitivity*. The composite measure of the size of a leak that a system can detect and the time required for the system to issue an alarm if a leak of that size should occur.

— *Accuracy*. The validity of leak parameter estimates such as leak flow rate, total volume lost, type of fluid lost, and leak location are indications of LDS accuracy.

— *Robustness*. The measure of the LDS' ability to continue to function and provide useful information even under changing conditions of the pipeline (i.e. transients) or in conditions where data are lost or suspect. A system is considered robust if it continues to function under less-than-ideal conditions.

9.2.3 Design of KPIs

KPIs can be designed for direct assessment and for diagnostic use. A KPI designed for direct assessment tells the operator if the performance target is being achieved. For example, if the performance target is no more than *X* alarms per month (not due to an LDS test or actual leak), then a KPI that counts the number of such alarms that occur directly indicates whether the target is being met. A KPI that estimates the amount of column separation (slack line) in the pipeline and counts the number of times it exceeds a threshold may be used as a diagnostic to explain why excessive alarms are occurring.

Many LDSs exhibit significantly different performance depending on the operation of a pipeline. Internally based LDSs such as CPM, for instance, are known to perform differently depending on whether the pipeline is shut down, operating in a steady condition, in a transient operation, during column separation, or at different flowrates. It may be useful to track each KPI separately for each operating regime to provide the data to make informed decisions about the performance of the LDS.

One possible way to assess the LDP and/or form a design basis for a LDP is to estimate the probability of detecting a leak as a function of time for a range of probable leak rates.

9.2.4 Examples of Metrics, KPIs, and Performance Targets

9.2.4.1 Examples Overview

This RP is intended to be general, focused on LDP issues, and not specific to a particular LDS. The examples given in this section are intended to clarify the issues of metrics, KPIs, and performance targets, and provide the framework of an operator’s leak detection performance and strategy. There are groups under the overarching metrics of the LDP but the list is not by any means exhaustive and is not meant to be prescriptive. Not all of the examples given would apply to all LDSs. Because actual leaks are rare, it is often feasible to track some of the following KPIs by validation testing.

9.2.4.2 Example Performance KPIs for Reliability

The following are a list of example KPIs which may be used to assess leak detection reliability. They may not be applicable to all LDS. Operators may track one or more KPIs for reliability.

— number of false positive indications per unit time (alarms/month), this may be tracked from observed data in normal operations.

— number of false negative indications (aka, f missed leaks) or percentage of missed leak events. This KPI may be expected to vary substantially with pipeline operation and somewhat with the location of the leak on the pipeline.

— count of leak indications without leaks (i.e., false alarms)

— count of leaks without leak indications (i.e., missed leaks)

9.2.4.3 Example Performance KPIs for Sensitivity

The following is a list of example KPIs which may be used to assess leak detection sensitivity. They may not all be applicable to every LDSs. These KPIs can be applied to each pipeline segment and / or observation time. Operators may track one or more KPIs for sensitivity.

— leak detection thresholds for a pipeline or pipeline segment. Users can track the minimum, maximum, or average thresholds, or a combination thereof.

NOTE Thresholds may be a useful proxy for sensitivity but due to the probabilistic nature of many LDSs, leaks greater than the threshold may not be detected, and leaks less than the threshold may be. This may be tracked from observed data in normal operations.

— minimum detectable leak sizes.

— time between the onset of a LOC and its detection. This is tracked separately for each leak observation time to detect for a fixed leak size.

— volume spilled before leak is alarmed.

— reliably detectable leak sizes.

NOTE Reliably detectable leak sizes are tracked separately for each leak observation time interval to assess sensitivity. It is theoretically possible that leak detection sensitivity metrics may be estimated by performing an uncertainty analysis of the algorithms used in the LDS.

9.2.4.4 Example Performance KPIs for Accuracy

The following example KPIs may be used to assess leak detection accuracy.

- Leak Flow Rate (Size) accuracy.
  - Many CPM systems compute a flow imbalance continuously with the imbalance in the flows compensated by the change in line pack. Since the sources of uncertainty such as instrument errors and unknowns in the pipeline operation are independent of a leak this is a useful proxy for the leak flow rate accuracy that may be observed during normal operation. This type of operation may be estimated using the techniques of API 1149.
  - For both CPM and non-CPM systems leak flow rate accuracy may be observed during leak testing.
  - For CPM systems this KPI may be expected to vary substantially with pipeline operation and somewhat with the location of the leak on the pipeline. To completely characterize the performance of a CPM LDS requires observing (or estimating) leak size accuracy at multiple operational conditions.
- for external system this metric will likely be more consistent for different operations and leak locations.
  - Leak volume accuracy. The same comments apply to leak volume accuracy as leak size accuracy, because the leak volume is just the accumulated leak flow rate.
- leak location accuracy.
  - Leak location accuracy may be observed for both CPM and non-CPM LDS's during physical leak testing.
  - This KPI may be expected to vary substantially with pipeline operation and somewhat with the location of the leak on the pipeline if a CPM is used.
- for external systems this metric will likely be more consistent for different operations and leak locations.
- diagnostic KPI's
- many leak detection systems such as Real Time Transient Model (RTTM) compute estimates of variables for which there are measurements, such as flow rates and pressures. Large deviations between these measured and computed values indicate performance problems with the LDS. While these do not directly relate to one of the metrics, they provide a useful diagnostic KPI.
- many leak detection systems such as an RTTM auto tune themselves by adjusting parameters related to pipe friction and heat transfer. When these parameters deviate from plausible ranges, it indicates performance problems with the LDS. While these do not directly relate to one of the metrics, they provide a useful diagnostic KPI.

9.2.4.5 Example Performance KPIs for Robustness

Leak detection robustness is concerned with the continued effective operation of the LDS.

Example robustness KPIs are:

- percentage of time at full performance;
- percentage of time unable to maintain full performance;
- percentage of time unavailable;

The factors which can inhibit LDS operations are virtually limitless. It is not necessary to correlate external events with robustness KPIs to effectively measure robustness.

9.3 Performance Targets

9.3.1 Defining Performance Targets

Performance targets define the expectation of an operator for an LDS or the specific implementation of an LDS on a particular pipeline based on the operator's risk tolerance. Performance targets for an LDS are used primarily when selecting which LDSs to have available in an LDP and for initial selection of candidate LDSs for a particular pipeline. Performance targets for a particular pipeline are appropriate for making final selection of an LDS for an asset and for evaluating continual improvement possibilities.

It is the intent of this RP to be general, focused on pipeline LDP management issues, and not specific to a LDS. To encourage some commonality between different LDSs, operators are encouraged to group their performance targets according to the performance metrics as previously discussed: sensitivity, reliability, robustness, and accuracy. It is possible that not all of these metrics are equally appropriate for every LDS.

Performance targets should be quantifiable and measured against KPIs. An operator may assign these metrics different importance according to the LDS or the asset to which it is applied. For example, an LDS intended for rupture detection has different metrics than one intended to identify small leaks.

9.3.2 Selecting Performance Targets

Care should be taken in selecting performance targets. The performance targets for an LDP may reflect:

— the operator's LDP strategy;

— the attributes of the LDSs ;

— the details of the pipeline or pipeline segment;

— the operator's risk profile

It may often be the case that an LDS may have multiple performance targets. This follows naturally from the aforementioned metrics of reliability, sensitivity, accuracy, and robustness that have been previously discussed. Multiple performance targets may arise in the context of evaluating different operating modes. Using CPM as an example, the sensitivity target during shutdown, steady state, and transient operations may be different.

With multiple performance metrics there is the possibility that conflicts may arise when setting targets. For most leak detection methods there is an inherent conflict between the sensitivity and the reliability. Where such conflicts are found to exist, priorities may be established to reconcile them.

9.3.3 Determination of Performance Targets

9.3.3.1 Determination Overview

Performance targets shall be determined using sound engineering expertise and judgment. Generic claims of performance by a vendor or other proponents of an LDS are not a substitute for systematic and engineering-based methods of establishing performance targets. Performance targets may be determined by estimation or observation of the LDS performance.

Performance estimation and observation are described in the following discussions. These techniques do not directly produce an appropriate value for a performance target. Rather they inform the operator on what may be reasonably expected from a LDS. For instance, an API 1149 analysis provides a theoretical best-case performance of a CPM system on a pipeline operating in nearly steady conditions. A CPM operating in transient conditions may not be capable of achieving this level of performance. Observing the same system's performance gives a figure that may be met but does not drive improvement. Knowing these numbers may assist an operator make a rational decision of what is likely to be an attainable goal for the LDS.

9.3.3.2 Determination of Performance Targets by Estimation

Performance estimation uses detailed knowledge of the LDS and how the inputs to and the operational environment of the LDS affect the performance. API 1149 is an example of this approach as it is applied to CPM LDSs. API 1149 contains an extensive discussion of the sources of uncertainties and how they affect leak detection performance. This principle may be applied to externally based LDSs. Annex C provides an example of uncertainties of four factors and demonstrates how they impact leak detection capability over various calculation windows. A operator may find it beneficial to perform these types of calculations to gain a better understanding of the capabilities of their LDSs. The fundamental principle of the output of API 1149 the LDS's sensitivity over time may be leveraged for both CPM and non-CPM LDSs. Performance estimation is appropriate where detailed and specific knowledge of the asset, the LDS, and the operations are available. This applies to assets that are installed or that have a detailed design available so that the specifics of the implementation are known. It implies that the methodologies of the LDS are known in sufficient detail to apply techniques such as uncertainty analysis.

The advantages of estimation are:

— may be performed before an LDS is implemented;

— allows comparison of different LDSs for an asset;

— provides prediction of the effects of changes to the configuration or operation of the asset or of the LDS.

The disadvantages of estimation are:

— the accuracy of the estimation is generally not known;

— when comparing different LDSs, if the difference in accuracy of the estimations is of the same order as the difference in the estimated accuracy, it provides no basis for selection and may even be misleading;

— the configuration of the asset should be known in detail, including items such as accuracy and precision of inputs that are difficult to obtain or assess;

— the physical principle of the technique used for the LDS should be known in detail however, this may not be available for proprietary technologies;

— derivation of the uncertainty relations for an LDS require a thorough understanding of the mathematics and statistics of uncertainty analysis.

9.3.3.3 Determination of Performance Targets by Observation

Performance observation uses analysis of historic performance of the LDS and/or testing that is designed to establish the performance of the LDS. Performance observation techniques are appropriate where detailed knowledge of the asset and its operation are known, and true performance is not known, so it should be determined for the existing asset and operation.

The advantages of observation are:

— it provides a definitive result for the performance;

— it accounts for as-built, real-world conditions.

The disadvantages of observation are:

— may not identify all factors limiting the performance;

— cannot be performed before an LDS is implemented;

— it does not provide predictive information on how changing the configuration or operation of the pipeline system may affect performance.

9.3.4 Additional Factors in Determination of Performance Targets

These two methods (estimation and observation) of determining performance targets are not exclusive. As an example, observation of the performance of a CPM LDS on a specific asset provides the definitive measure of the performance of the LDS. A performance estimation technique may be used to estimate the performance that may be expected if the operation or configuration of the asset is to be changed. An performance estimation analysis might be used to determine if the observed performance is expected or if the observed performance indicates a problem with the LDS Sound engineering practice and experience is used when deciding whether a difference in the estimated and observed performance of an LDS is attributable to inaccuracies inherent to the estimation procedure or if additional investigation is warranted.

A special case of using more than one method (estimation and observation) is to use observed performance to “tune” or history match the inputs to the estimation technique to cause it to calculate the observed performance. Without great care, such an exercise may produce inputs to the estimation procedure that match the observations used to tune the LDS but may not produce the correct results when used to estimate the performance of the LDS with new operations or configurations.

9.3.5 Developing Performance Targets for LDSs

Both estimation and observation are useful to determine, or at least estimate, the performance of a specific LDS applied to a specific asset. They may be applied to generalize about the performance of an LDS by performing the analysis for many pipelines with common characteristics, such as all those that use an LDS. For instance, an operator may deduce that their uncompensated volume balance CPM achieves X % sensitivity versus Y % for their compensated volume balance. Such a finding is obviously a simplification since each pipeline has a unique performance, but generalized metrics may be useful in many instances such as making an initial choice of an LDS for an asset.

10 Testing

LDSs used in an LDP shall be tested when implemented and on a regular basis or when there has been a significant change which may impact the LDS, or when deemed appropriate by the operator. The testing should be tailored to accommodate the unique aspects of the LDS and the specific assets on which the LDS is implemented. Actual leaks or expected maintenance or operational activity driven alarms (filling equipment, relief valve activation, etc.) may be used in lieu of periodic testing.

Possible methods of testing include but are not limited to:

— removal of test quantities of commodity from the line.

— editing of configuration parameters or inputs to simulate commodity loss or a desired hydraulic condition.

— create inputs to simulate commodity loss for an external LDS.

Altering an instrument output that is critical to the LDS: e.g. altering a meter factor to simulate a volume imbalance, or a pressure output to simulate a hydraulic anomaly. Wherever possible the testing should incorporate the recommendations of the LDS manufacturer or developers. The use of the manufacturer’s recommendations may be critical to performing an effective test of the LDS.

A test plan should be prepared prior to testing. The test plan should document the purpose of the test, the methods to be employed, and the process and procedures that should be followed. LDS tests should be rigorous and be planned and executed using sound engineering and technical judgment. The test plan should be consistent with the operational and safety policies of the operator.

The operator may leverage LDS system tests to test staff who respond to leak alarms. Examples of tests include:

— does the staff know the procedures for responding to leak alarms,

— how they respond to non-leak alarms and true leak indications,

— how they respond to anomalies that may indicate a leak,

— how they respond when the LDS is degraded or has failed.

The operator may use the results of performance testing for opportunities to improve the equipment, culture, procedures, and knowledge levels. This may provide feedback to LDP training. Knowledge or skills acquired in training are tested as a part of the training program.

11 Control Center Procedures for Recognition and Response

11.1 Overview of Procedures

The operator shall provide a documented leak response procedure to be used in the case of a leak indication on the pipeline. This procedure should be complementary to an operator's existing emergency response procedures, providing additional guidance that is specific to a leak response situation. During a leak indication, a Controller may need to reference this procedure to ensure that the proper actions are taken.

The Controller is an important component in the loop of responding to the LDS alarms. Operators should explicitly declare the level of individual authority and responsibility of Controllers when a leak alarm is initiated. Operators may have additional personnel available who are dedicated to supporting the Controller to analyze alarms and monitor the system.

When developing and maintaining a recognition and response procedure for Controllers or other Control Room personnel, there are a number of best practices that may be utilized when a leak indication occurs. This section provides examples of these best practices and guidance for implementing them.

An operator's leak detection culture should reinforce the idea that all leak indications have a cause and should be evaluated. The leak response procedure should outline the processes, tools, and actions that should be used by the Controller to recognize and respond appropriately to various leak indications. These procedures should be constructed with a consequence-based mindset, with directives for acting in the event of a leak indication. Procedures should be clear for ease of understanding by the Control Center personnel and concise for ease of use.

The use of flow charts may help clarify the actions specified in the written procedures. The operator's leak detection culture and training should ensure that the procedures are followed.

11.2 Recognition of a Leak Indication

A correct and timely response to a leak indication is dependent on a Controller's successful recognition of the conditions that indicate Loss of Containment (LOC). To that end, there are a number of indications that may initiate a leak response. The term "leak indication" does not always mean that an actual leak has occurred. What it does mean is that an alarm or other notifying event has occurred that suggests that present conditions indicate the possibility of a leak and that immediate action is required by the Controller.

The operator should develop procedures for indications or combinations of indications. There may be many types of LDS alarms or leak indications. The Controller should be able to recognize the indication of a potential leak and then use the prescribed tools and techniques to respond accordingly.

Alarm handling is discussed in detail in API 1167, Section 9.

11.3 Response to a Leak Indication

A leak indication should compel a Controller to take immediate action. The Operator may specify different actions to respond to different leak indications. For example, an operator's leak response procedure may dictate that certain leak indications require an immediate shutdown of the pipeline while other indications may dictate that the Controller take additional action to analyze the current pipeline operation or escalate the investigation to other SMEs to determine the cause of the leak indication before a shutdown is required.

The indicated magnitude of the leak, the persistence of the leak indication, the number of independent indications, leak location, and the level of risk involved may be factors in determining the action a Controller should take as documented in the operator's leak response procedures.

The response may differ based on the characteristics of the pipeline on which the indication is noted and the indication type received (i.e. some indications require a limited period of analysis before a shutdown, others may require an immediate shutdown). In general, leak indications are announced through LDS-generated alarms, recognized through data analysis (hourly reports, pressure trends, etc.), or based on reported evidence of a leak (field surveillance identifies product in ROW, dead vegetation, neighbor reports smell of gasoline, etc.).

11.3.1 Leak Indications Requiring Immediate Shutdown Response

The first category of response is to alarms or indications as determined by the operator's procedures which require an immediate shut down of the pipeline.

Operators should be clear in their procedures about when a pipeline is to be immediately shutdown following a specific leak indication.

11.3.2 Analysis of a Leak Indication

The operator's procedures should specify different actions that are taken to analyze different leak indications. Therefore, it is imperative that the Controller correctly recognize the indication of a potential leak or use a team approach.

During the analysis, the Controller/team should implement one or more of the following:

— follow procedures as written;

— utilize operator-provided analysis tools (e.g. hydraulic calculations, trending, etc.);

— utilize additional expertise (perhaps as a team effort with others such as leak detection analysts or senior Controllers);

— ensure that leadership is taken by one person;

— evaluate the information provided by complementary or alternative LDS;

— recognize conflicting data, and how those data may influence the analysis;

— increase level of scrutiny where there are low credibility alarms or work is being performed on the line;

— know what to monitor and look for, and what tools to use;

— whenever possible, use an independent means of verifying the cause of the leak indication (the operator designates what constitutes an independent means);

— apply their knowledge of the function of the LDS or technique that alarmed;

— during the analysis, apply their knowledge of the unique operating aspects of the pipeline that has the alarm;

— with caution, recognize that leak indications may be attributed to non-leak reasons.

Depending on the operating conditions and the nature of the leak indication, it may not be immediately apparent that an actual LOC has occurred. Most leak indication responses that do not require an immediate shutdown of the pipeline involve a limited period of analysis during which the Controller checks a variety of conditions that may have triggered the alarm (data failure, irregular operating condition, etc.). The leak response procedure should include methods (for example, pressure trend analysis) and tools (for example, a hydraulic calculator) to aid in determining the cause of the leak alarm. During this period, the Controller may request team support to analyze the leak indication and document the actions.

11.3.3 LDS Indications Prompting Additional Analysis

An operator may have a second category of response where alarms, notifications, or a combination of indications require timely investigation and preparation for potential shutdown or other actions. These instances include but are not limited to the following:

— indications at an intermediate location that are not supported by overall hydraulic conditions (i.e. flow upstream and downstream are correct).

— loss of function of the leak detection technique (e.g. heartbeat alarms).

— communications outages at time of alarm.

— data or instrumentation fault.

— data or instrumentation outage alarms.

— notifications from surveillance or third-party reports.

— a CPM deviation warning (not all LDSs have these type of alarms) that indicates a deviation that is not yet above leak threshold.

— alarms that occur while calibration or other work is occurring on the pipeline in the area of the work.

— manual method (non-CPM) deviations such as over/short calculations that are not supported by leak detection alarms.

— alarms that cannot be verified by call-outs in field.

— visual sensors indications.

— surveillance leak indications with no show of hazardous liquid or related effects (i.e. vegetation indications).

— alarms that occur when a new batch is introduced.

— alarms that occur when a new or unusual flow path is used.

— alarms that coincide with start-up/shutdown or rate changes.

— instances where pumps shut down automatically or may not start due to low pressure.

— when set point changes are made.

— abnormal operating conditions; for example, radical unexplained pressure/flow deviations.

— alarm repeats.

— SCADA rate-of-change alarms or indications.

— column separation indications that are occurring where it is an unlikely possibility.

— power outages at the time of an alarm.

For leak indications that do not require an immediate shutdown of the pipeline, the leak response procedure may specify a predefined time limit or volumetric limit to investigate the leak indication before further action is initiated. The operator may specify different time limits or volumetric limits for each individual pipeline LDS or for the sake of simplicity may define a single limit. In either case, the limit specified should be based on rational analysis of the pipeline LDS to ensure a safe and timely response. The Controller is not required to wait for the time limit to expire or the volumetric limit to be exceeded before acting. If the Controller has sufficient reason based on the available information and tools to suspect that a LOC has occurred, they shall take immediate action to respond to the leak indication.

If the analysis and investigation find that the cause of the leak indication was confirmed to be some condition other than a LOC, the indication may be cleared, and the pipeline may resume normal operation.

11.3.4 Mitigating actions to a leak indication

When either the initial analysis of the leak indication has concluded, or if the time limit or volumetric limit to determine the cause of the leak indication has expired, or the leak indication requires a controller action, the Controller should take the appropriate action, which may include escalation, based on the analysis and the leak indication.

Leak response procedures should recognize that a leak indication may be triggered from several different sources. The procedures should characterize the leak indicators to the best extent possible so that common language is used. Through procedures and training, Controllers should have a detailed knowledge of their role and responsibilities during a leak indication response.

A typical response procedure should include directions to take actions that the operator deems to be safest and most appropriate for the pipeline in question. Controllers should be empowered to shut down and isolate the pipeline segment in a safe and controlled manner where the leak is suspected to have occurred.

Operator response procedures should also include contacting emergency officials or 911 services when warranted.

Further investigation of the leak indication and operational data may continue until independent leak verification has been confirmed or disproved. This may include a field visual assessment of the affected assets and/or an asset integrity verification procedure.

11.4 Validating the Leak Indication

Leak validation is triggered by the suspicion that a leak exists and examines the pipeline and/or analyzes pipeline operation data in order to verify and make a formal determination of the existence of a leak or alarm cause verification. Examples of leak validation/cause verification may include, but are not limited to:

— hydraulic calculations,

— pressure and flow monitoring (trending),

— CPM LDSs,

— externally based real-time LDSs,

— real-time video feed that is continuously being analyzed,

— aerial surveillance,

— ground surveillance (foot patrol),

— internal pipeline inspections,

— external pipeline inspections,

— pressure testing (shut-in testing/stand-up testing) where this is possible.

11.5 Reporting and Documentation

During and/or after a leak indication the actions taken should be logged. The abnormal operating condition and actions taken to mitigate the issue should be logged per an operator's response procedures. Log details can include, but are not limited to:

— event timeline and duration,

— classification of the indication,

— date/time of the indication,

— location of the indication on the pipeline,

— what triggered the leak indication (which may be unexplainable),

— hazardous liquid being transported,

— consequence/impact of the indication,

— pipelines and facilities involved,

— actions taken in response to the indication.

For a confirmed leak, the operators should document additional information. This information can include, but is not limited to:

— information from Field Operations;
— emergency notifications issued with date and time;
— chronology of communications between stakeholders;
— teamwork participants during the analysis;
— reporting agencies contacted date and time;
— estimated leaked volume;
— flow logs of a duration to cover before and after the indication;
— pressure logs of a duration to cover before and after the indication;
— temperature logs of a duration to cover before and after the indication;
— pump statuses and valve position logs of a duration to cover before and after the indication;
— alarm/events logs and trends;
— Controller logbook/notebook and turn-over logs;
— SCADA and leak detection data capture;
— cause of the event (human error, faulty equipment, leak, pigging operation, column separation, drag reduction agent (DRA), atypical operations, new commodity, etc.);
— which LDS detected the leak;
— leak source and component;
— other data related to the leak and its detection;
— contributing factors
— other data as required by the operator’s emergency response plan.

The documentation may be used by the operator’s investigation team to thoroughly investigate the events and take the appropriate actions to identify and address the leak indication. The documentation is also used in alarm management (see 12).

11.6 Pipeline Restart

Operators should develop a procedure for restarting the pipeline following a shutdown driven by an LDS indication.

The procedure can contain requirements for restart, which can include physical/visual inspection, shut-in testing/stand-up pressure monitoring for a predetermined amount of time, or other appropriate sources or methods of ruling out a leak condition.

The operator should maintain a high level of awareness when a pipeline that has been shut down is restarted. Extra attention should be given by both field personnel and the Control Center staff during and after the restart process to help confirm the absence of a leak. This restart procedure is not a part of detecting the leak but should be part of Control Center procedures.

Restart documentation may include a checklist. This checklist is to be used to verify that the issue has been resolved and that it is safe to restart the line.

11.6.1 Pipeline Restart after no evidence of a LOC

Operators should develop a procedure for restarting the pipeline following a shutdown where no evidence of LOC was detected.

After a leak indication analysis where no evidence of a leak is confirmed, a controller can restart a pipeline using the operator's restart procedures.

11.6.2 Pipeline Restart following a confirmed LOC

Operators should develop a procedure for restarting the pipeline following a shutdown where there is a confirmed LOC.

The restart process should consider any required regulatory action associated with the event such as a corrective action order. A pre-start-up safety review may be needed if any modifications (permanent or temporary) have been made to the system. The operator's procedures and appropriate stakeholders should be engaged and formal documented approval granted before any restart is authorized.

12 Alarm Management

12.1 Alarm Management Purpose

The purpose of alarm management is to only permit genuine, actionable alarms to be delivered to the operator / controller.

Alarm management employs data collection, review, and validation. It may make use of statistical alarm techniques and advanced analysis. Alarm management should encompass methods aimed at increasing Controller responsiveness by increasing confidence in the LDS performance.

See API 1167 for additional information on alarm management.

12.2 Data Collection

Alarm data collection requires the gathering of all the information that was recorded during the handling of the alarm and adding to that information additional data that may be used during alarm review.

Alarm data collection and categorization evaluates post-alarm actions to capture the information recorded at the time the alarm occurred and to add additional information to create an accessible history of leak alarm information and build an alarm history that may be used for alarm review. Immediate handling of leak detection alarms is the function of the Control Center procedures outlined in the previous section.

The alarm data collection should record information on the Control Center response to the alarm. This information can be used to inform improvements to the LDP.

12.3 Categorization

Alarm causes should be determined or confirmed for relevant alarms so that improvements may be made. Responses to alarms should be categorized. Example alarm response categories include:

- alarms that required immediate action to shut down the pipeline;
- alarms that required an immediate investigation and preparation to shut down;
- alarms that were proven to be non-leak alarms following a review.

This may be the desired way to divide alarms for the Controller, but further categorization may aid in the review process and in improving the LDS (i.e. increased granularity is desirable).

Other possible alarm categories or subcategories may be cause-based—examples are as follows.

- data failure
- operational issues

Tunable or Sensitivity issues where the non-LOC alarms that were generated may be prevented by some form of tuning/adjustment to an LDS, Table 3 is an example of information that may be useful in alarm data collection or in the alarm review that follows but is not all encompassing.

Enough information should be captured so it is possible to determine what adjustments may be made to improve the leak detection alarms and response.

Table 3—Example Alarm Categorization Table

Category	Definition	Response	Further information
Leak	LOC	Followed Procedure	Location, size, cause
Expected Field Work	Alarm due to field work with prior knowledge	Followed Procedure	What was being worked on
Infrequent Operation	Alarm due to new or infrequent operation	Followed Procedure	What is different or new
Instrument Failure	Alarm due to instrument failure	Followed Procedure	What failed
Column Separation	Column separation causing an alarm	Followed Procedure	Start-up or flowing with column separation
No Call-in	Alarm due to field work with no prior knowledge	Followed Procedure	What was being worked on

12.4 Alarm Review

Alarm review is the process of analyzing data collected about alarms (see 12.2) with the goal of increasing the confidence in the LDS. The alarm review should evaluate the KPIs associated with the leak alarming and may point to possible further action (e.g. threshold setting) or improvements within the operator.

12.4.1 Goals

The goals of alarm review should be to look for improvement possibilities, which can include:

— learning opportunities (for the Controller, SCADA, engineering, field operations personnel, HSE (health, safety, and environment), compliance, and any other relevant stakeholders);

— LDS configuration changes;

— new equipment or instrumentation;

— KPI validation (15.4);

— LDP changes (which may include adding alternate or complementary LDS methods).

12.4.2 Periodic Review

The operator should conduct short- and long-term alarm history reviews to develop strategic plans for continuous improvement.

12.4.2.1 Short-term Periodic Review

The purpose of the short-term review is to determine how the LDSs are performing and the operator's response. The short-term review may include:

— review program KPIs and trends to determine where immediate corrective or improvement action should be taken;

— reviewing of responses to the alarms and the procedures.

The result of this review may result in actions or recommendations intended to improve the accuracy, reliability, and robustness of the LDS.

Attention should be paid to how the results of short-term periodic review feeds into the long-term periodic review. This feedback may influence the frequency of the short-term periodic review. Operators should establish a regular review schedule for their LDS, but this may change based on short-term requirements.

12.4.2.2 Long-term Periodic Review

Periodically, with the time between reviews not to exceed five years, the operator should complete a review of the alarm performance and thresholds of each LDS. The purpose of this review is to assess the alarm performance and thresholds from the perspective of sensitivity and reliability, and the appropriateness of the thresholds of the LDS with respect to the KPIs and performance metrics.

The frequency of the long-term periodic review should be a risk-based analysis. This frequency may be uniform for all pipelines or may be pipeline dependent. This risk-based analysis can include the following:

— operator's risk tolerance,

— frequency of major/minor changes on the pipeline,

— frequency of testing,

— complexity of pipeline operations,

— presence of occasional column separation operation,

— LDS KPIs

— robustness of the process control system or network.

The operator should determine which KPIs defined in 9 should be used as part of this long-term periodic review. The operator should define the measures to evaluate each KPI and the data collection method and frequency for those measures.

The long-term periodic review may also include:

— actual leaks;

— withdrawal tests;

— simulated testing;

— stakeholder reviews;

— equipment additions/replacements;

— leak detection method additions/replacements;

— operational changes (alarm response, avoiding column separation, etc.);

— KPI updates.

For example, the classification of the alarms and alarm codes may be the result of the short-term periodic review.

The operator should document the results of the long-term periodic review.

12.5 Confirmed Leak Review

In the event of a confirmed leak, the LDS shall be analyzed, the response of the LDS evaluated, and the result documented. This may be an opportunity to review the response of the Control Center to the leak. The result of the LDS is dependent on the characteristics of the leak. General classifications for review of actual leaks may include classification by the following:

Within LDS scope:

— the leak signature is significant enough to be detected by the LDS, but the LDS failed to detect the leak;

— the LDS successfully detected the leak.

Out of LDS scope (outside of the physical boundaries of the LDS; example: upstream of an injection flow meter):

— leak rate is small enough that there is no observable leak signature in the LDS input data;

— leak rate is small enough that the leak signature is indiscernible from typical system noise.

If the LDS successfully detects a leak, an analysis shall be performed as there may be valuable lessons learned, training opportunities, or areas of improvement identified.

If the LDS failed to detect a leak that is within the scope of the LDS, an investigation shall be performed to determine the cause and identify if any corrective actions should be taken. The investigation can include review of previous non-leak alarms on the pipeline segment, functioning of the LDS during normal operations, and verification of all configuration parameters. The investigation may include a review of possible issues with data communication to or from the LDS software or issues with SCADA pre-processing of data used by the LDS.

The operator should make changes if warranted, and test to verify the leak detection method is functioning as intended.

The alarm review may indicate tuning rather than threshold adjustment if the investigation warrants it. The alarm review may indicate having dedicated LDS alarm analysis personnel to relieve the Controller of the LDS alarm burden, having improved sensitivity, and documenting the reason(s) for the alarm notification.

12.6 Threshold Setting

12.6.1 General

Threshold setting involves adjusting the detection threshold level to alter the LDS performance. Threshold setting may involve the tuning of several parameters which can impact the sensitivity or speed of detection for certain leak sizes. Note that threshold setting only applies to systems that have the feature of adjustable thresholds.

Threshold setting evaluates the existing thresholds and, based on an alarm review, the need for adjustment of the thresholds to maintain the performance according to the specified or expected metrics of sensitivity, reliability, robustness, and accuracy. Threshold setting acknowledges the expected thresholds from the selection, the cause of the alarm, and what process may be undertaken to adjust any thresholds to ensure the required metrics and KPIs based on operator’s culture and strategy are achieved or maintained. Alarm threshold settings should not be adjusted outside the range of upper and lower design limitations.

Threshold setting acknowledges the threshold expectations of the LDS, performance monitoring results (particularly test results), and input from the Control Center to set detection thresholds for those LDSs that have adjustable thresholds. Threshold setting should be aligned with the operator’s leak detection strategy.

There is a trade-off between reliability and sensitivity. As sensitivity is improved, reliability may be decreased, i.e. there may be an increased number of false alarms. The adjustment of leak detection thresholds to reduce the sensitivity and increase reliability of the leak detection method may be done in conjunction with the addition of complementary LDSs to compensate for the reduced sensitivity. A higher alarm rate may be acceptable if good diagnostic tools are provided or if additional information is provided that may be used to verify or disqualify alarms.

Non-leak alarms beyond the KPI value set (see 15.4) may be a driving factor in determining if adjustments are needed to the LDS.

12.6.2 Threshold setting philosophy

Threshold setting may use the following:

— *Reliability-focused philosophy:* define a tolerable alarm limit (i.e. a targeted number of alarms) and adjust thresholds until you hit the alarm limit. This may result in poor sensitivity.

— *Sensitivity-focused philosophy:* define sensitivity targets and set thresholds to meet those targets. This may result in poor reliability.

— *Balanced philosophy:* Set both alarm limits and sensitivity targets. If both cannot be met through threshold tuning, other methods may be required to reach targets, such as new instrumentation, hydraulic model tuning, or operational changes.

Leak indication thresholds may be changed or adjusted on a temporary basis. Operators should document these changes and follow their MOC process.

Dynamic thresholds, a type of threshold adjustment, may be utilized provided they are understood. Dynamic changes to the threshold should be available to the Controller. This may be a primary feature of the LDS where the LDS dynamically adjusts the threshold to provide large volume leak detection during transitions of flow and pressures during the pipeline operation, which are typically during pipeline startup or shutdown.

Short-term threshold changes to suppress alarms by threshold adjustment should be discouraged. However, maximum limits for adjustment may be established and there should be a threshold notification to alert the Controller that an adjustment is active. There should also be a process that returns the threshold to normal. The supervisor should be advised that the threshold will be or has been manually adjusted and the reasons why. The time the adjusted threshold was in effect should be logged. The supervisor's approval may be required.

12.6.3 Threshold setting to reduce non-leak alarms

The operator may implement changes that do not adjust the thresholds before permanent threshold changes are contemplated. To reduce non-leak alarms, possible changes can include:

— equipment preventative maintenance or replacement (failed pressure or temperature probes);

— modification of operation (minimize column separation conditions; for example, by maintaining a packed pipeline on shutdown or packing a pipeline before beginning operation);

— tuning the leak detection parameters (see 12.7);

— instituting dynamic alarm thresholds within the leak detection alarming schema.

NOTE Dynamic alarms adjust thresholds, but only on a temporary basis. The primary or steady state threshold is not changed.

12.6.4 Threshold setting review

Before changing leak detection thresholds, there should be a review process that may include, but is not limited to, the following.

— Determining if thresholds are too tight vs. too loose

— Evaluating operational changes to reduce impact on leak detection, e.g. change an operation that causes alarms.

— Determining if the alarms are due to some normally recurring conditions.

— Weighting short-term vs. long-term review input.

— Providing or receiving feedback to or from Control Center.

— Finding changes that do not affect the leak detection technique.

— Determining if a complementary LDS or enhancement to the LDS may solve the uncertainty.

— Ensure that proposed changes are in line with strategy.

— Review the applicability of a proposed threshold change on a particular LDS.

— Perform calculations to determine what may be the required change.

The operator should use procedures for any threshold change and it is particularly important that they inform the Controller and Control Center of any changes.

NOTE See 17 on management of change for additional information

Rupture alarm thresholds are a special case. Rupture thresholds are set to alarm with high reliability.

API/AOPL White Paper 12, *Liquid Pipeline Rupture Recognition and Response* (August 2014) contains a discussion on this rupture thresholds.

12.7 Tuning

Tuning is adjusting the leak detection technique for more precise functioning, or target performance per the operator's strategy. Tuning is normally undertaken when an LDS is initially installed and may continue for some time. Tuning may occur when changes are made to leak detection inputs, the operation of the line changes, or to improve sensitivity or reliability of the LDS. Tuning is a valuable process in which one or a number of tuning factors are changed and evaluated. Tuning may be performed by the operator or by the LDS vendor. If the operator undertakes the tuning, the methods suggested by the vendor may be used as a guide. It is critical that as-existing tuning factors and as-changed tuning factors are recorded. The effect of the tuning on LDS performance should be monitored, and the results should be documented. Tuning may involve repeated iterations until the desired performance level is achieved.

During tuning, other changes to the LDS system may be required, for example, repair of instrumentation or sensors. Implementing data filters to prevent some alarms may be a form of tuning.

Tuning is not calibration but can achieve improved performance. Most often, tuning is applicable to CPM LDSs but may also be applied to externally based LDSs. CPM LDSs often have many tunable factors and the tuning involves changing the weight of one factor in relation to the others. Tuning may be pipeline-specific, so even if the same LDS is used on various pipelines, the tuning factors may be different. Optimally, LDS tuning is performed offline with a data set large enough to encompass expected seasonal and flow regime variations.

13 Roles, Responsibilities, and Training

13.1 Roles and Responsibilities

Operators should have clear descriptions of their leak detection stakeholders' roles and responsibilities. This helps the stakeholder(s) understand their areas of responsibility and the operator's expectation(s) of them. Clear descriptions of roles and responsibilities allow the individual and/or group to understand how they support the leak detection strategy and where they contribute to the leak detection culture.

Operators may have the same name for the same functions (i.e. Controller because it is a common title). However, different titles are often used for others who are involved with leak detection and have different responsibilities for employees even when the same function title is used. Because of these differences, it is not possible to accurately describe the roles and responsibilities for all employees and stakeholders. The roles and responsibilities titles and descriptions used in this section are examples only. A brief description of the roles of those involved in leak detection and a list with many of the common titles related to leak detection that are used is shown in Annex E. These are listed in relation to the department, section, or functional area where they are often used.

For the various LDSs in use by the operator, there may be additional and specifically defined roles and responsibilities for the staff that use and support that leak detection method.

Operators should track and communicate to internal stakeholders changes to leak detection roles and responsibilities.

13.2 Training

13.2.1 General

An effective training program has the potential to greatly reduce the consequences of a pipeline leak, particularly at the Control Center level.

Personnel who interact with any part of an operator's LDP should receive initial training, retraining, and refresher training.

The specific level and the content of training received may be based on the role that an individual has in the operator's LDP.

See Annex F for an example of a training program, listing of the level and content of training recommended for each role, and recommended training delivery and testing/verification methods.

13.2.2 Roles and Training Content

Each operator should define the role requirements based on the size and complexity of its pipelines and LDP (see Table 5). For this section, the roles and training content used in Table 5 are examples.

NOTE External stakeholders such as landowners, emergency officials, and public officials are generally not included in training programs and are made aware of leak detection and response through operator public awareness programs.

Table 5—Role and Content of Training

Role	General Training Content
Management	Culture, Management, Reporting, Broad Operational, and Broad Technical
Control Center	Culture, Management, Reporting, Detailed Operational, and Broad Technical
Analyst: Leak Detection Staff	Culture, Management, Broad Operational, and Detailed Technical
Engineering: Support Staff	Culture and Detailed Technical
IT Group	Culture and Detailed Technical
SCADA Support	Culture and Detailed Technical
Field Operations: Field and ROW Staff	Culture, Reporting, and Area-Specific Technical
Field Operations: Connecting Facilities Staff	Reporting and Area-Specific Technical

13.2.3 Leak Detection Drills

Running leak drills prepares personnel to work efficiently and effectively as members of a group. The emphasis during leak drills is on effective communications amongst stakeholders who would be involved in leak indication investigation.

Drilling as a team in an exercise that includes pertinent levels of authority as may be defined in a response procedure is important. The team is presented a scenario and is to respond using associated documentation and/or procedures.

The parties involved may include: Control Center staff, support staff, field staff, management, and external emergency support response. In addition, there may be simulated reporting, coordination, and interaction with government agencies, regulators, and the public.

A tabletop format may be used with all players in a single room, or a combination of tabletop and field exercise may be appropriate. The intent is to train, evaluate, and improve response as an integrated team in as realistic an environment as possible.

The importance of clear and unambiguous communication should be stressed during drills. Drills should test and emphasize the abnormal and emergency roles and functions of the personnel involved in the exercise. The scenario should test the effectiveness of procedures for elevating the Controller's support beyond the Control Center within the time constraints of those procedures. One of the best techniques for reinforcing effective human factors practices is careful debriefing of the exercise and highlighting the processes that were followed.

13.2.3.1 Groupthink

Evaluation of the team's performance during the exercise should include an assessment of the degree to which the team avoided engaging in groupthink. Avoiding groupthink is important in the early diagnosis phase of a leak and during the entire response phase. The longer a response takes, the greater the possibility that groupthink may occur.

Groupthink is often without critical evaluation of alternative viewpoints, actively suppresses dissenting viewpoints, and isolates the group from outside influences. Groupthink may be evident by loss of a sense of vulnerability, complacency, or an environment that supersedes the authority of the Controller and does not allow for independent decisions to be made.

A SME in organizational behavior may be employed to observe and evaluate the exercise to detect this phenomenon and the interpersonal communication, leadership, and decision-making during the exercise.

13.2.4 Training Frequency

13.2.4.1 Establishing Intervals and Extent

The operator should establish an interval for retraining and refresher training, as well as outline the extent of training for personnel who interact with the operator's LDP.

13.2.4.2 Refresher Training

Refresher training is an abbreviated form of the initial training and is independent of retraining. The primary audiences for refresher operational and technical training should be Control Center staff and leak detection staff. Operators may establish refresher training frequency for roles receiving leak detection basics and awareness levels of training. Decision factors for refresher training may include:

— size and complexity of the operator's pipelines and LDP;

— a leak indication or drill;

— a fixed frequency for Control Center and LD staff, particularly for alarm attribution skills;

— leak drill exercises at regular intervals.

13.2.4.3 Retraining

Retraining is completion of some or all parts of the LD training program for the role and may be used for an individual who has been out of a role for period defined by the operator. For Controllers, that period should match the period that the operator established under its OQ program for other qualifications.

14 Reliability Centered Maintenance (RCM) for Leak Detection Equipment

14.1 Maintenance Overview

Operators should establish written policies and procedures to ensure that components of the LDS and their supporting infrastructure components are designed for reliability and maintained appropriately.

The maintenance should cover both externally based and internally based LDSs and all components associated with LDSs in use by the operator. These components include field measurement and instrumentation, communication systems, processing units, and backup systems.

The process should include scheduled maintenance that is a part of an operator's policy and existing RCM program. There should be a process for immediate maintenance and repair of LDS components that have failed or are providing inaccurate or "bad" readings. Sometimes the LDS behavior is the best indication when maintenance is required. The maintenance plan may call for servicing instrumentation when the LDS behavior, limits, or output are affected.

"Reliability" for equipment is defined as the likelihood of a failure occurring over a specific time interval. "Availability" is a measure of equipment being in a state of readiness for its intended task. "Maintainability" is the parameter concerned with how the equipment in use may be restored after a failure, while accounting for concepts such as preventive maintenance and diagnostics (built-in tests).

14.2 RCM Process

During the maintenance planning process, it is necessary to discuss the maintenance program with the users of the LDSs and/or with vendors.

The maintenance program and process may include the following questions:

— What is the function of the item or component and what is its associated performance standard?

— In what ways may it fail or degrade? What are the events that cause each failure\degradation of that component?

— What happens when each failure\degradation occurs?

— In what way does each failure \ degradation matter to the LDS?

— What procedures may be implemented to prevent consequence of failure \ degradation (an active prevention approach)?

— What may be done if a suitable preventative task cannot be found?

— What is the impact on the LDS during maintenance activities and what procedures should be followed?

These facets co-outline an RCM process and align with FMEA approach. A useful reference is SAE JA101, *Evaluation Criteria for RCM Processes*.

14.3 Leak Detection Component Identification

Leak Detection equipment which is integral to the reliability of a LDS should be identified and documented. These components may be physically tagged and/or their corresponding tracking database tags identified to indicate that they are components of the LDS.

API RP 1130 addresses CPM instrument identification.

14.4 Design

LDSs shall be designed for Reliability, Availability, and Maintainability.

Redundancy for component failure and maintenance may be provided. This may be hardware redundancy for individual components, backup systems, communication channels, or alternative operating procedures. For example, redundant sensors may be made active while the primary is offline for calibration, maintenance, or replacement. The operator may evaluate the process by which a redundant system or component becomes active. An automatic cut-over to the backup/redundant system or component is one approach. Use of an alternate operating procedure is another approach.

Field instrumentation should be appropriate for the task and design specifications should provide for the required accuracy. Program policies may specify design requirements of instrumentation. As an example, measurement accuracy and repeatability should be specified to meet appropriate targets for leak detection. LDSs should be able to maintain specified performance under all operating conditions and not just when conditions are ideal.

14.5 Maintenance Tracking and Scheduling

The operator should integrate maintenance of the leak detection components into an operator's Maintenance Management System (MMS) or Computerized Maintenance Management System (CMMS) or similar system to provide for automation of maintenance activity and failure tracking. A CMMS may include the ability to capture reliability metrics such as Mean Time Between Failure (MTBF). These reliability metrics may then be evaluated to determine if additional action is needed to prevent future LDS component failures that would adversely affect leak detection performance. Reliability metrics may be tracked for both communications and processing unit components (e.g. communication losses to field instruments, or net server up time).

CMMS may include ties to a MOC process. When a MOC process is not linked to the maintenance system, then some type of MOC process should be applied.

The operator should provide for scheduled (i.e. routine) calibration and make allowance for unscheduled (i.e. break-fix) activity and the device criticality ranking. The schedule may be time based or based on some other criteria, for example: proving may be performed for each batch. Some components of a LDS are more critical than others. Each operator may create a ranking system (i.e. through RCM) for each component and specify the impact of a component failure and provide clear policies for actions to take when a device is compromised. Criticality is determined by the effect the loss of the device (or the associated loss due to degradation) has on the leak detection technique. For example, complete loss of a flow meter in a volume balance CRM may cause a total loss of function of the leak detection technique, while varying accuracy of a flow meter may reduce the effectiveness of the technique but may not make it inoperative.

By tracking reliability metrics for field instruments and other LDS equipment, communications, and processing units, a strategic plan may be implemented to address issues and drive for a more reliable LDS. These reliability metrics should be linked to the operator's performance metrics, KPIs, and targets.

Additional maintenance and reliability should include software maintenance (e.g. patches, revision, updates, code fixes, etc.) if necessary. Clear policies and procedures should be in place to ensure that the required maintenance is properly communicated to appropriate stakeholders as to duration, impact, and effectiveness. Potential risks should be identified and communicated.

15 Overall Performance Evaluation of the LDP

15.1 Purpose and KPIs

Overall LDP performance evaluation focuses attention on the LDP management program results that may demonstrate improved safety and risk reduction has been attained. The measures provide an indication of effectiveness, but are not absolute. Performance measure evaluation and trending may also lead to recognition of unexpected results that may include the recognition of threats not previously identified. All valid performance measures are simple, measurable, attainable, relevant, and permit timely evaluations. Proper selection and evaluation of performance measures is an essential activity in determining leak detection program effectiveness

The overall performance evaluation of the operator's LDP should capture and evaluate noteworthy results of operation of the LDP, benchmark company performance, and report to management on a periodic basis the results of the overall performance monitoring. The overall performance evaluation should be performed using an internal review.

An external review can also be performed, if sufficient relevant data is readily available, in addition to the internal review.

The operator should establish KPIs that can be used to measure the overall performance of the LDP. The LDP's performance can be measured against targeted performance or against historical performance.

15.2 Internal Review

Operators should establish a comprehensive internal data repository or enhance existing data repositories to facilitate the data collection and analysis process.

The results of the internal review can include:

— identified gaps in strategy;

— performance metrics evaluation results;

— assessment of the strength of the culture;

— changes to roles and responsibilities;

— new activity in the selection process;

— performance monitoring and target changes;

— testing/tuning results;

— feedback from the alarm management process;

— training results;

— notable equipment maintenance activities;

— MOC measures;

— improvements suggested, undertaken, and completed.

15.3 External Review

External comparisons may provide a basis to evaluate the performance of the LDP management program. The purpose of the external review is to seek benchmarking information and improvement possibilities.

The information may be:

— leak indication reports;

— regulator databases (e.g. PHMSA, NEB);

— guidance provided by regulators and others;

— activities in the pipeline industry;

— changes to regulations and any other related sources.

Benchmarking with other operators may be useful; however, any performance measure or evaluation derived from such sources should be carefully evaluated to ensure that comparisons are valid.

15.4 Key Performance Indicators (KPIs)

The leak detection strategy may have performance requirements for the overall LDP and KPIs are used to measure progress against those requirements.

Performance measures are selected carefully to ensure that they are reasonable program effectiveness indicators. Change should be monitored so the measures remain effective over time as the plan matures. The time required to obtain sufficient data for analysis may also be considered when selecting performance measures.

The steps to define KPIs for an organization start with a solid understanding of the processes in use by that organization to achieve its objectives. In the LDP, this process starts with an understanding of the leak threats and the leak consequences to be able to develop an appropriate strategy, which may then be used to identify appropriate LDS selection and implementation. Overall monitoring of all aspects of an LDP may be realized through defining the correct KPIs and collecting the data consistently, reporting properly, and acting on the data once it is evaluated.

The steps are:

— process review,

— define KPIs and review,

— collect data,

— reporting,

— analysis,

— corrective action.

The review may separate the findings into categories of leading and lagging indicators and further into levels as outlined below (see Figure 3).

Leak detection systems uses four metrics to rate performance. These four metrics are: accuracy, sensitivity, reliability, and robustness. However, additional KPIs should be defined to monitor the overall effectiveness of the LDP. The first step in defining LDP KPIs is that the operator should understand the process that is followed in defining, implementing, and executing the LDP. KPIs may be identified to understand if the process is functioning in alignment with the overall goals and the specific outcomes desired from the LDP.

Each operator should develop their own list of KPIs.

15.5 Periodic Reporting

Well-designed KPIs are useful measures for the operator's personnel to understand how well the people, processes, and LDSs are functioning to achieve the overall objectives that have been approved as part of the leak detection strategy. As such, there should be a reporting of the most significant KPIs to the operator's management on a periodic basis. The management review should include documentation that the review occurred.

15.6 Leading and Lagging Indicators

15.6.1 Review Process

There are several concepts that should be understood prior to implementing a set of KPIs to measure the success of an LDP. Of particular importance is the difference between leading and lagging indicators. Lagging indicators are "after the fact" measures, whereas leading indicators can help companies take a more proactive stance in managing their LDP.

15.6.2 Lagging Indicators

Lagging indicators are those KPIs that measure an event after it has already occurred.

An example of a lagging indicator is a measure of how many pipeline leaks were alarmed by an LDP that includes at least one LDS that was designed to detect a leak of that size in a given time period.

15.6.3 Leading Indicators

Leading indicators are used to give advance indications of the potential effectiveness of an LDP before an incident. These are valuable to define, measure, and evaluate if a process is working currently and/or will work correctly during a future incident. An example of a leading indicator is a measure of how Controllers are trained in the use, understanding, and operation of the LDSs implemented within a Control Center. The underlying assumption is that well-trained Controllers would be better able to understand the data being presented to them and respond in a more appropriate manner. Therefore, a KPI to reflect this may be the percentage of Controllers who are trained on the concepts of the LDSs on a periodic basis.

It is important to note that the delineation of leading and lagging indicators is contextual and dependent on the end use of the indicators themselves. Summarily, the same indicator could be leading or lagging under different conditions and use of the same.

15.6.4 Dual Assurance

Dual assurance is a concept whereby a leading indicator is organically matched with a lagging indicator. An example of this relationship in an LDP would be a leading KPI to measure the percentage of non-leak alarms that are analyzed, rationalized, addressed, and documented by the leak detection compared to a lagging indicator where a Controller's shutdown percentage in response to leak alarms is measured. The assumption being that a more careful, thorough evaluation of non-leak alarms by a leak detection analyst and tuning of the LDS would result in a lower number of unwarranted shutdowns.

15.7 LDP KPI Examples

The following are examples of LDP KPIs, which have been categorized for the user's convenience:

15.7.1 Post-LOC KPIs

These KPIs are directly tied to some measure of an LOC.

— barrels per leak where continuous LD method was designed to identify leak

— what LD methods detected the leak

— estimated total cleanup costs to operator resulting from LOC where a continuous LD method was designed to identify the leak

— time between LOC and leak alarm, where continuous LD method was designed to identify leak or notifications

— number of large leaks where continuous LD method alarmed, where continuous LD method was designed to identify leak

— percentage error in identifying the leak location by the LDS, where continuous LD method was designed to identify leak

— number of leak events where the LDS did not alarm when the continuous LD method was designed to identify the leak

15.7.2 Implementation KPIs

These KPIs are more operationally focused and emphasize the challenges to the particular LDS(s) implemented by the operator.

— number of alarms that are received by the Operations Center in each time period

— number of false alarms generated from the LDS

— amount of time that an LDS is in alarm state during operation

— percentage of leak alarms where the cause of the alarms or notifications is identified, i.e. communication, metering, instrumentation, SCADA, abnormal operations, physical environment etc.

— percentage of total pipeline covered by a continuously monitored LDS

— percentage of total pipeline where actual LDS performance meets design criteria

— percentage of time that the LDS is available during operations (uptime of the LDS)

— number of tests conducted on an LDS in a given period

— percentage of LDSs with non-tuned thresholds

— percentage of LDSs that undergo a periodic review of alarms or notifications

15.7.3 Process KPIs

These KPIs are generally leading KPIs and are more focused on measuring the quality of the processes used within the LDP:

— percentage of Controllers who are trained on the concepts of the LDS and company/operator response procedures on a periodic basis

— average percentage of time LDS operates in a degraded status

— percentage of MOC items that impact the LDP

— percentage of LDSs where alarm settings are reviewed and confirmed on a periodic basis.

16 Controller Training and Retraining

Controllers and any leak detection support staff require appropriate training. LDS alarms may be the most complex type of alarm experienced by the Controller. This requires both a knowledgeable perspective on the alarms themselves as well as the nature of the alarms.

The training plans may include;

— periodic reviews and or knowledge testing of the Controller.

— review of training material to be accurate and thorough.

Retraining may be aided by review of known cases where the irregular operating condition alarms or abnormal operating conditions have occurred, and possible commodity release alarms have been generated.

16.1 Hydraulics

Controllers should be trained in the basic concepts of pipeline steady state hydraulics as they relate to the LDS system. This knowledge can include the variances of hydraulic pressure due to elevation profiles, batches of differing density, temperature effects, and DRA. Controllers should also be trained in the basic relationship of pressure and temperature during shut-in conditions.

Controllers should be trained to recognize the effects of pump start-ups/shutdowns, valve operation switch, pressure setpoints and other everyday activities, which cause transient conditions. Any of these will cause a system flow or pressure transient to appear potentially affecting CPM thresholds leading to non-leak alarming.

16.2 Alarming/Performance

Controllers should be able to recognize and react to all LDS alarming, cognizant to indicators of LDS system performance.

16.3 Data Presentation

Controllers should be trained in the recognition of the LDS notification or alarm and may be trained to research the cause of the alarm (data failure, irregular operating condition, or possible commodity release), or in methods of correlation of the alarm to independent data so the Controller will pursue the appropriate response. The presentation of alarm data is a crucial component, such as the trend of the probability of a leak, or the description of the location for which the leak declaration has occurred.

Other specifics to data presentation can be referred to in API RP 1165.

16.4 Instrument Failure

Controllers should be able to qualitatively identify the impact of an instrument failure on the LDS system. Controllers should be trained to link the alarm event with the concept that the LDS system could be impaired.

16.5 Validating LDS Alarms

An evaluation of the LDS system and operating conditions is necessary for validating or explaining the cause of aN alarm. Controllers should be trained to recognize and react to abnormal operating conditions and to take appropriate action. The training may be directed towards following procedures or calling upon and working with external resources for alarm evaluation.

16.6 Line-pack Change (Online)

Controllers should be trained to recognize CPM hydraulic pressure changes due to varying line-pack. A fundamental element in the spectrum of inventory control is the calculation of mass, or the comparison of barrels in versus barrels out. This training would include the ability to recognize the compressibility behavior of the liquid hydrocarbons that are transported.

Controllers should be knowledgeable about sections of the pipeline that are susceptible to intermittent “slack line conditions.” Controllers should be knowledgeable about how this condition affects the CPM performance.

16.7 Trending

Controllers should be able to recognize benefits provided by trending analysis of pipeline variables from SCADA. Trending data can be presented graphically or as a tabular display of historical data. A graphical output may provide the best visual history of LDS parameters. Controllers should be able to cross correlate LDS output with SCADA output wherever possible confirming alarm evaluation.

16.8 LDS System Operation

Controllers should be trained to understand the LDS, and the concept/theory of its operation. A portion of Controller training may include periodic review of the use of the LDS in a training environment. Training may cover all the various LDS in use within the Control Center and unique aspects of each application as they apply to individual pipeline segments.

Controllers should be trained to interpret alarms correctly and in a timely manner or work with internal or external resources to evaluate the alarm. The LDS should be implemented so the alarms are readily recognizable.

16.9 Abnormal Functions

Controllers should be trained to recognize and react to the abnormal function of a LDS as well as the abnormal function of the SCADA system. The loss of either should elicit certain predefined actions intended to preserve pipeline integrity. Targeted response actions should be thoroughly analyzed and scripted for prompt, efficient action.

For example, if the LDS becomes non-functional or severely degraded due to field equipment or SCADA failure, the Controller should be trained to employ other leak detection methods to compensate for the inadequacies of that LDS. Alternatively, the Control Center can to define what interval of time the LDS can be non-functional and what action should be taken. Short term solutions may consider manual line balance and over-short and Pressure/Flow Monitoring. Actions might include tightening of pressure and flow alarm parameters.

16.10 Other Leak Detection Techniques

Controllers should be trained in how to employ the results of other leak detection technique such as third-party reports, SCADA deviation alarms, etc. so that a particular LDS is not considered to be the only means of detecting leaks. Controllers should know what procedures to follow and reactions to make for other methods.

17 Management of Change (MOC)

Operators shall apply their formal MOC process as required per local governing regulatory agency to any aspects of LDSs (technical, physical, procedural, and organizational) that change. The MOC process should include the requirements of API 1160, API 1167, and API RP 1173. The requirements of the three API standards may be tailored to accommodate the unique aspects of LDSs. Changes to leak detection programs which directly impact control room operations or alarming should follow API 1167 and 1168.

18 Improvement Process

18.1 Overview of Improvement Process

An ongoing improvement process is an important part of the LDP and should align with the operator’s strategy. Suggestions for the LDP improvement process are provided in this section. The improvement process itself should be reviewed on a regular basis. KPIs that are specific to the improvement process should be tracked and reviewed for progress. The improvement process should define improvements in the LDP, plan for and track to completion tasks that are needed to meet existing LDP goals, or to satisfy new goals.

Improvement of the operator’s LDP and strategy involves two aspects: identifying and defining issues for improvement and initiating and monitoring the improvement process for the identified issues. The results of improvements undertaken and/or the improvements underway should be reported periodically.

18.2 Identifying and Defining Opportunities

Improvement issues and suggested improvements should be identified during the management of the LDP. The operator should develop a plan or process to capture improvement suggestions so they may be used to manage the improvement process. The issues identified should be described by the party who identifies the concern and the issue should be passed into the improvement process. It may be possible to establish metrics and KPIs that may be used in evaluating the continual improvement possibilities.

The improvement process may start with the following information.

- Suggestions or requirements for improvement of the LDP.
- Suggestions or requirements from 15.
- Any new continual improvement targets or information that may be used to set new continual

improvement targets (benchmarking, etc.).

— Applicable standards and industry best practices.

— Details of previously identified actions for improvement with their status (determine if previous actions are being properly executed. If not, adjustments should be made to ensure execution of the actions).

Possible items for inclusion in an improvement process can include:

— Information provided in the overall LDP evaluation and covering LDP KPIs .

— Lessons learned from the review of industry leaks or leak alarms (where these exist).

— Issues encountered in the maintenance programs and analysis (i.e. worst actor/bad actor, updates to the FMEA).

— Gaps identified by KPI evaluation, event analysis, Root Cause Analysis (RCA), where parts of the LDP failed.

— Gaps identified in the strategy, selection, or the work of any other section outlined in this RP.

— Performance monitoring results as recommended in the performance-related sections in the RP.

— Trends indicating issues with the operator's leak detection capability or effectiveness.

— Operator performance comparisons or benchmarks.

— Results from examination of software upgrades.

— New detection techniques that offer features that promise improvements to the LDP.

— Engineering studies (possibly including API 1149 calculations) that indicate where other instruments or more measurement may be beneficial.

— Information obtained at conferences or from conference papers, R&D programs, results of R&D tests, etc. that may be applicable.

— Results of tests that indicate disconnect between expected and actual performance.

— Information on frequency of threshold adjustments.

— Information about new shipping routes or products.

— Issues about unclear roles and responsibilities that should be clearly defined.

— Issues about unclear Control Center recognition and response or LDP procedures.

— Changes related to updated risk analysis, meaning the risk has changed.

— Training concerns.

— Perceived level of commitment to the LDP within the organization and things being done to retain commitment to the LDP.

— Changes to or evolution of regulations.

— Issues with public perception of the operator's system.

— Issues identified or indicated in the integrity management plan.

Annex A
(informative)

Risk Assessment

A.1 General

The risk assessment may include consequences, likelihood/threats, frequency, and other risk factors associated with leak detection and identified in the IMP.

A.2 Consequence Analysis

A consequence analysis (comparing mitigated and unmitigated consequences) of a hazardous liquid LOC may include the factors outlined in Table A.1.

Table A.1—Consequence Factors

Pipeline profile
Terrain surrounding the pipeline
Flow path for leaked hazardous liquid
Waterways, streams, ditches, and subsidence areas that may act as a conduit to a high-risk area
Hospitals, care facilities, schools, and retirement homes
Population density
Places where people congregate
Commercial navigable waterways
Drainage systems or conduits
Land usage (farm field, urban)
Fish hatcheries
Fluid characteristics and leak potential/volume
Detection time
Possible size of leaks
Dispersion path of any flammable vapors
Dynamic and static leak volume
Distance between isolation points or valves
Cost of cleanup
Health, Safety, and Environment (HSE) factors
Existing LDP, principles, methods, and techniques
Number of primary and complementary LDSs and their capabilities
Response time at all levels
Response capability in field
Pipeline accessibility
Type of valves: motorized EFRDs, hand-operated valves, remote control valves, automatic control valves

Time required to isolate the pipeline segment or contain the hazardous liquid leak
Pipeline system hydraulics and operation
Emergency response plans
LOC scenarios
Pristine areas that are SAs

The operator should define the response time and the steps. It would typically include the total time of multiple steps; for example: time to detect, time to analyze and verify, time to shut down and isolate, and perhaps time to get response people to the leak site.

A.3 Likelihood/Threat Analysis

The likelihood of different leak rates occurring depends on the likelihood of initiating events, meaning how likely and perhaps how often they occur. The primary possible causes or threats of a pipeline failure that results in a leak are outlined in Table A.2.

Table A.2—Likelihood Factors

History of leaks on the pipeline
Corrosion
Equipment failures associated with pipeline appurtenances
Incorrect operations/human error (e.g. exceeding MOP MAOP)
External damage caused by operator personnel, contractor, third party, etc.
Manufacturing defects
Subsidence, soil washout possibilities
Construction defects
Weather or outside forces
The deliberate action of outside agents for either commercial reasons (theft) or political/motivational reasons (terrorism)
Other/unknown
Other likelihood factors
Potential natural forces inherent in the area: flood zones, earthquakes, slide areas
Pipeline characteristics
Throughput
Physical support of the segment such as by a cable suspension bridge
Non-standard or other than recognized industry practice on pipeline installation
Pipeline integrity issues
Results from previous testing/inspection
Known corrosion/condition of pipeline
Cathodic protection history
Type and quality of pipe coating
Age of pipe
Type, growth rate, and size of discovered defects/anomalies

Frequency of inspection/testing (or time since last inspection)
Internal testing
Pressure testing
External inspection
Operational factors
Stress levels in the pipeline
Exposure of the pipeline to an operating pressure exceeding the established maximum operating pressure
Quality of MOP estimates
Intermittent column separation

A.4 Preventative Factors (Protective Layers)

Various preventative factors are outlined in Table A.3.

Table A.3—Preventative Factors

Pipe: wall thickness (WT), cathodic protection (CP), coatings, anomalies/defects, wall-loss rate, corrosion rate
Overpressure protection: maximum operating pressure (MOP) vs. normal operating pressure (NOP) alarms, thermal reliefs, pressure reliefs, safety instrumented systems (SIS), back pressure control system (BPCS), critical alarm panels, pipe casings
Damage prevention: One-calls, third-party prevention, community awareness, 2nd-containments, design for natural disasters, sabotage/vandalism/terrorism prevention
Inspection practices: in-line inspection (ILI), risk analysis, repair programs, CP programs, surveillance, ROW monitoring, public awareness
Corrosion: design, inhibitors, ground beds, rectifiers
Escalation barriers
Bored or open cut under-river installation

A.5 Risk Analysis and Evaluation

Other factors that are likely included in the IMP analysis and may be included in leak detection method selection are outlined in Table A.4.

Table A.4—IMP Factors

Repairs (type and time since completed)
Defects: found, causes, degradation
Pipeline attribute changes
Re-alignment with inspection findings
Results of preventative and mitigative measures (PAMMs)
IMP history

Annex B
(informative)

Developing a List of Selection Criteria

B.1 General

Developing a list of selection criteria can help satisfy problem solution, strategy, risk tolerance, and regulatory requirements. There are two key areas: what features are needed and what performance is required. These are discussed below.

B.2 Features Desired

The physical environment in different areas may impact features and an operator's decision on the best method(s) to implement. There is no reason why such features may not be used for the entire pipeline system, but practicality, risk, and other factors would come into play deciding the best method(s) to use. The physical environment in different areas may impact these features and a operator's decision on best method(s) to implement them.

The features listed (in no particular order) in Table B.1 are in addition to those outlined in API 1130. In some cases, they may be a near-repeat of API 1130 items or an expansion of the API 1130 list.

Table B.1—LDS Features

Supportable at minimum cost and effort
Utilizes instrumentation currently installed and/or minimizes additional
Internally based or externally based
Suited to existing data acquisition rate
Technology available, industry proven, convenient
Continuous vs. non-continuous nature of the method
Dependent vs. independent methods for each LDS on a pipeline
Commonly used with other pipelines
Alarming ability
Tunable features
Adjustable thresholds
Minimal complexity of training required for the users
Maintenance and support activities available within operator
Fits evergreen activities within the operator
Diagnostics tools are available in the method (i.e. not a black box)
Fits with operability and business continuity planning
Implementation ease
Growth potential for the future
Additional desirable features that may be useful (e.g. trend charts)
Lifecycle maintainability (includes all costs)
Operator's experience with the application

Testability (there is a concern about testing some externally based methods) in service

Table B.1—LDS Features (Continued)

Testable while being implemented and deployed
May be enhanced from basic configuration (e.g. infrared sensors added to visual methods)
Upgradable (more features may be added)
Minimization of technological complexity
Covers all pipeline physical characteristics
May operate with elevation profile and profile accuracy
Suitable for ambient temperatures
Low frequency of configuration changes
Suitable for pipeline network complexity
May operate with power/infrastructure available at sites
Suitable for burial depth of pipeline
Works with soil characteristics
Able to operate with weather patterns along pipeline
Operates with all pipe equipment: valves, stations, segments, stub lines, dead legs
May accommodate physical properties of hazardous liquid
Works with SCADA system
Specifically for a RTTM
Handles pressure/temperature transients
Handles column separation/slack line operation
Fully covers throughput ranges from maximum rate to shutdown
Items that are part of the pipeline operational characteristics
Handles frequency of startup/shutdown (strong transient events)
Handles imposed flow transients
Able to handle flow direction changes
Other factors related to the feasibility of the method
Cost
Procurement ease
Installation ease
Maintenance required
Additional staffing requirements
External support requirements

Table B.1—LDS Features (Continued)

Works with existing infrastructure (both back office and field)
May use current measurement and instrumentation
Power additions required

Personnel knowledge base needed:
Other selection factors. These are listed in no particular order
Whether the various LDSs have a single common point of failure (i.e. part of independent or dependent)
Whether there is a sufficient user base to ensure that the vendor is long term viable and stable
Amount of training required for the configuration staff and users
Whether a risk-based evaluation can be used
For a non-continuous or periodic LDS, the minimum frequency and whether that frequency appropriate for the particular pipeline
Whether the LDS has suitable diagnostic tools not only for alarm analysis but also to evaluate if it is operating at 100% of capabilities
Amount of maintenance required to ensure the LDS remains operable
Display capabilities of the LDSs
Whether the LDS is testable with the existing resources
Types of tools or methods needed to confirm the cause of the alarm
Whether the LDS can be easily tested during selection evaluation
Offline capability for training (provided as standard with software)
Whether the LDS can be implemented in a simple configuration, then upgraded with additional incorporated features later
Whether API 1149 calculations can be applied to estimate the capabilities of the LDS
Types of leak validation methods that should be used to evaluate alarms (e.g. on-site inspections, use of experts, pressure testing)
Applicability to the full range of the operator’s pipelines and products
How a particular leak detection methodology may complement another methodology
Existence of other potential benefits, such as communication possible through fiber optical cables
Whether instruments should be relocated for optimal LDS performance or the existing sensors as situated are suitable for the LDS

B.3 Performance Desired

Evaluations for performance required/desired and for selecting the leak detection principles, methods and techniques that are used in the operator’s LDP may require a comparative evaluation of the performance wanted and the performance possible. The performance may be quantified by use of metrics and related KPIs.

For the purposes of understanding performance, the aspects of an LDP may be categorized as monitoring, surveillance, or verification. Leak detection monitoring is performed on a continual basis with the intent of detecting operational or physical changes of a pipeline segment that may indicate that a leak has occurred. In order to classify as monitoring, a component should be actively “watching” for the formation of a leak, typically using real-time data or other means.

Examples of leak detection monitoring are shown in Table B.2.

Table B.2—Types of Leak Monitoring

One-call notifications
Public awareness capabilities
Rupture monitoring LDSs

Line patrol and surveillance leak monitoring
Pressure and flow monitoring
CPM LDSs
Externally based real-time LDSs
Real-time video feed that is continuously being analyzed
Visual detection by company employees or contractors

Leak detection monitoring may be characterized using the following performance indicators of Table B.3.

Table B.3—Monitoring Performance Indicators

Sensitivity of threshold detection
Frequency of monitoring
Reliability of the LDS

There are typically multiple components of an LDP that work with each other to reduce the detection time. During the LDP design and management, it is useful to also evaluate the combined effects of the LDS components.

The likelihood of the success of the monitoring is a combination of the reliability and robustness. Leak detection surveillance examines the pipeline on a periodic basis in order to determine if a leak exists.

Examples of leak detection surveillance are shown in Table B.4.

Table B.4—Types of Surveillance

Leak surveys
Long-term inspections
Aerial surveillance
Foot patrol
Internal pipeline inspections
External pipeline inspections

Annex C
(informative)

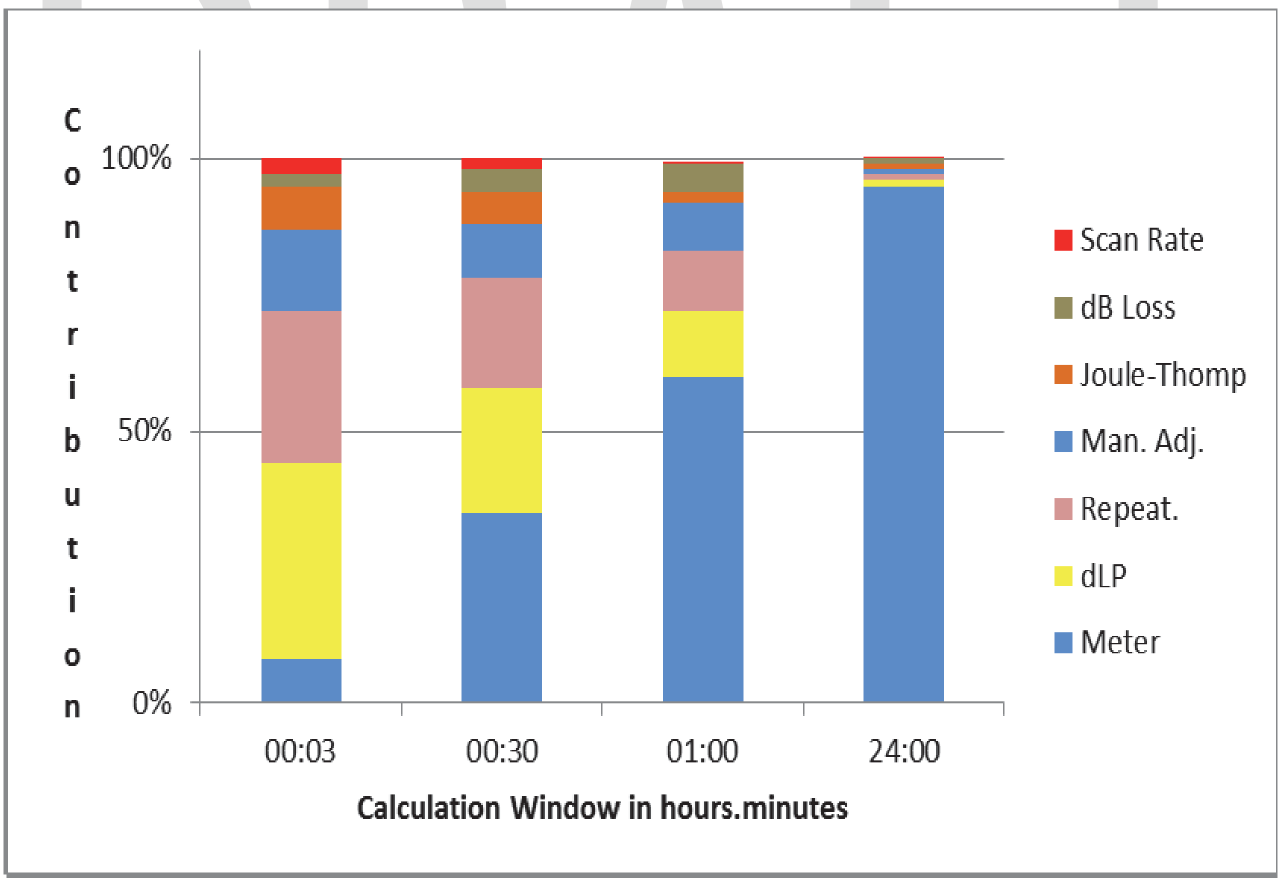
C.1 Factors Affecting Performance

Figure C.1 represents an example only of the effects of only seven of the various types of uncertainties in the leak detection inputs and illustrates how each affects performance in the various calculation windows that are used in this example LDS for a particular pipeline.

In this figure: Scan Rate is the SCADA scan rate; dB loss is the signal-to-noise ratio of the sensing element; Joule–Thomp is the Joule–Thompson effect of the fluid temperature to soil/ambient temperature (typically applies to HVL lines); Man. Adj. is manual adjustment (a threshold factor utilized by the operator (in bbls); Repeat. is the repeatability of the meter (in bbls); dLP is the change in line pack error (in bbls); and Meter is the meter error (in bbls).

In a short leak detection window, the meter accuracy has less impact on performance (less than 10 %, the dLP has a large impact (about 36 %), the repeatability has a moderate impact (about 28 %), and the Man. Adj. has a moderate impact (about 15 %). For a 24-hour leak detection calculation window, almost all the performance uncertainty is attributable to the meter accuracy.

Figure C.1—Effects of Uncertainty Types



Annex D
(informative)

Example of Performance Metrics and Targets

Table D.1 indicates performance metrics and targets that operators might apply to a pipeline with a CPM LDS. In the far left column are the leak detection goals. The second column gives the metrics or KPIs that are being tracked. Columns 3, 4, and 5 give the performance targets for each metric. There are three performance targets in recognition that the expected performance of a CPM LDS differs in different flow regimes. The last column indicates how the performance target was determined. The possibilities in the example are as follows.

— observed/historical—the target should be determined by analyzing historical data from the LDS during actual operations.

— observed/testing—the target should be determined by analyzing data obtained from a test of the LDS.

— estimated/API 1149—the target should be determined by using uncertainty analysis techniques as detailed in API 1149 to estimate the expected performance of the LDS.

Table D.1—Example Performance Metric/Target Table

Goals	KPI	Operation			Notes
		Shut-in	Steady	Transient	
Reliability	Non-leak Alarms	< 1 per month for all operations			Obs./Historical
Sensitivity	Average Alarm Threshold	10 bbl/30 min	100 bbl/30 min	500 bbl/30 min	Obs./Historical
		20 bbl/1 hr	200 bbl/1 hr	1000 bbl/1 hr	Obs./Historical
		40 bbl/2 hrs	400 bbl/2 hrs	4000 bbl/2 hrs	Obs./Historical
Accuracy	Leak Flow Rate	No Target	± 20 bph	Not Determined	Obs/Testing
	Leak Location	No Target	± 5 miles	Not Determined	Obs/Testing
Robustness (Reliability)	Non-leak Alarms During Comm Fail	No Increase			Obs./Historical
Robustness (Sensitivity)	Degradation in Average Alarm Threshold due to Missing Pressure Measurement	100 %	0 %	25 %	Est./API 1149
	Degradation in Average Alarm Threshold due to Missing Flow Measurement	0 %	100 %	100 %	Est./API 1149
Robustness (Accuracy)	Degradation in Leak Flow Rate Accuracy due to Missing Flow Measurement	No Target	No Target	No Target	No Target
	Degradation in Leak Flow Rate Accuracy due to Missing Pressure Measurement	No Target	No Target	No Target	

NOTE The volumetric values listed in this table are for example only and may not have any physical reality to a particular pipeline.

Table D.2 indicates performance metrics and targets that a pipeline operator might apply to a pipeline using external method LDS. The table below shows an example for fiber optic sensing. Similar to CPM, the far left column describes the leak detection goals. The second column gives the specific metrics or KPIs that are being tracked. Columns 3, 4, and 5 give the performance targets for each metric. There are three performance targets in recognition that the external LDS method may be used in conjunction with a CPM LDS. The last column indicates how the performance target was determined. The possibilities in the example are as follows.

— observed/historical—the target should be determined by analyzing historical data from the external LDS during actual operations.

— observed/testing—the target should be determined by analyzing data obtained from a test of the LDS.

Table D.2—Example Performance Metric/Target Table

		Operation			
Goals	**KPI**	**Shut-in**	**Steady**	**Transient**	**Notes**
Reliability	Non-leak Alarms	< 1 per month for all operations			Obs./Historical
Sensitivity	Average Alarm Threshold	0.5 bbl/15 min	0.5 bbl/15 min	0.5 bbl/15 min	Obs./Testing
		1 bbl / 30 min	1 bbl / 30 min	1 bbl / 30 min	Obs./Testing
		2 bbl / 1 hr	2 bbl / 1 hr	2 bbl / 1 hr	Obs./Testing
		4 bbl / 2 hr	4 bbl / 2 hr	4 bbl / 2 hr	Obs./Testing
Accuracy	Leak Location	± 10 meters	± 10 meters	± 10 meters	Obs./Testing
Robustness (Reliability)	Non-leak Alarms During Comm Fail	No Increase			Obs./Historical
Robustness (Sensitivity)	Degradation in Average Alarm Threshold due to Cable Cut	0% before cable cut location, 100% after cut location. (Or) 0% degradation for cable cut robust configuration.			Obs./Historical
	Degradation in Average Alarm Threshold due to field interrogator failure.	100% degradation for the segment monitored by the failed interrogator. (Or) 0% degradation for redundant interrogator configuration.			Obs./Historical
Robustness (Accuracy)	Degradation in Leak Location Accuracy due cable cut	0% before cable cut location, 100% after cut location. (Or) 0% degradation for cable cut robust configuration.			Obs./Historical
	Degradation in Leak Location Accuracy due to Interrogator Failure	100% degradation for the segment monitored by the failed interrogator. (Or) 0% degradation for redundant interrogator configuration.			Obs./Historical

NOTE: The volumetric values listed in this table are for example only and may not have any physical reality to a particular pipeline
Leak flow rate accuracy is not a KPI for fiber optic sensing-based LDS.

Annex E
(informative)

Common LDS Roles

E.1 General

Each operator may use different names or have different roles for the staff involved in use and support of the LDSs. This annex provides a brief description of roles and a list of common names used by operators.

E.2 Controllers

Controllers remotely monitor and control the operations of entire or multiple sections of pipeline systems via a SCADA system from a pipeline Control Room and who has operational authority and accountability for the daily remote operational functions of pipeline systems.

Controllers may defer action to others but are still the primary responsible individuals monitoring and detecting abnormal conditions. Controllers utilize automation and tools to determine if a LOC is occurring. Controllers communicate with and assist field personnel during the investigation of a leak indication. Controllers have the authority to shut down any pipeline and/or device without prior approval when they suspect a leak or there is an abnormal or emergency condition. They are the primary investigators of leak alarms. They are also the primary recorders of information about leak alarms, although all staff have some role and responsibility for record-keeping and reporting requirements. Other commonly used names used for Controllers are shown in Table E.1.

Table E.1—Other Commonly Used Names for Controllers

Console Operator	Operator
Dispatcher	Pipeline Controller

E.3 Leak Detection Analyst

Leak detection analysts analyze data provided by SCADA, leak detection software, and/or personnel to determine if there is a leak and work with the Controller. Leak detection analysts provide procedures for pipeline operation as it relates to leak management and provide additional support to Controllers who shut down pipelines when there is uncertainty. They also manage the development and maintenance of leak detection operating and maintenance practices and procedures. Other commonly used names for leak detection analysts are shown in Table E.2.

Table E.2—Other Commonly Used Names for Leak Detection Analysts

SMEs	Operation Center Analysts
On-call Support Staff	

E.4 Leak Detection Engineers

Leak detection engineers design and implement LDSs. They work with the Control Center, field operations, and SCADA support on maintenance and updates of the LDS and manage efforts to improve the LDS capabilities, including the evaluation and implementation of value-adding LDS improvements. Leak detection engineers also provide computerized LDSs in accordance with business and regulatory requirements. Other commonly used names for leak detection engineers are shown in Table E.3.

Table E.3—Other Commonly Used Names for Leak Detection Engineers

Hydraulic Engineer	SME
Project Managers	Metering Specialists
Measurement Engineers	Automation and Hydraulic Engineers
Measurements Specialists	Leak Detection Engineers
Leak Detection Architect	Measurement Staff
Measurement and Material Balance Specialists	Capital Project Engineers
Control Engineers	Control Specialists
System Planning Engineers	Engineering Staff
Technical Advisors	

E.5 Control Center Staff

Control Center staff communicate with and assist operational personnel. They work with engineering and SCADA support on maintenance and updates of the LDS and communicate with and assist operational personnel in responding to or investigating a leak, or any operator personnel who are involved in identifying, detecting, reacting to, or notifying of a leak. Other commonly used names for Control Center staff are shown in Table E.4.

Table E.4—Other Commonly Used Names for Control Center Staff

Supervisors	Shift Supervisors
Leads	Managers/Directors
Control Center or Operation Center Staff	Control Center Management
Control Center Supervisors	Operation Center Analysts
Operations Center Supervisors	Operations Center Specialists
Leak Detection Staff	Leak Detection Analysts
On-call Support Staff	
CPM Engineers	SMEs
Leak Detection Engineers	Asset Integrity Engineers
Surge Analysts	Schedulers
CPM Analysts (including Vendors or Consultants who fill the role or any individual in the decision loop)	

E.6 Field Operations

Field operations include all of the operator’s staff who work at locations along the pipeline. This category may include the following: contractors, third party operators, or any other personnel not described as an operator or full-time personnel who share the same responsibility as the department and position they serve. They may be part of the team that approves pipeline re-start after a leak detection-related shutdown. Other commonly used names for field operations staff are shown in Table E.5.

Table E.5—Other Commonly Used Names for Field Operations Staff

Field Operations and Maintenance Personnel	Operations Technician
Operations Supervisor	Operations Superintendent
Area Manager	Regional Manager
Field Engineers	Electricians
Gaugers	Instrumentation Technicians
Tank Farm Staff	Surveillance Personnel
ROW staff	Internal Emergency Responders

E.7 Information Technology

Information technology provides support to leak detection equipment and some aspects of software such as computer equipment, corporate connections, databases, secure access, etc. Other commonly used names for IT staff are shown in Table E.6.:

Table E.6—Other Commonly Used Names for IT Staff

IT Staff	IT Support

E.8 Leak Detection Trainers

Leak detection trainers ensure that Controllers are appropriately trained and qualified to operate the pipeline including operation of the LDS. They develop and execute an appropriate training and qualification program and ensure that leak detection analysts are appropriately trained and qualified to provide required Controller support and required LDP management. Other commonly used names for trainers are shown in Table E.7.

Table E.7—Other Commonly Used Names for Trainers

Leak Detection Trainers	Control Center Trainers

E.9 Management

Management approves the operator's leak detection strategy and provides leadership, support, and resources for achieving their organizational goals. It manages the definition and execution of required LDP system maintenance and management practices and procedures to maintain required levels of LDS performance and reliability. Management also defines LDP support personnel requirements and ensures appropriate availability of qualified LDS support personnel, as well as defining business requirements for LDSs. It maintains awareness of regulatory requirements for computerized LDSs and ensures that LDSs are managed to maintain compliance. Other commonly used names for management are shown in Table E.8.

Table E.8—Other Commonly Used Names for Management

Senior Management	Supervisors
Middle Management	

E.10 Leak Detection SCADA Support

Leak detection SCADA support staff implement automation of engineering design and communications to the leak detection hardware/software at operational locations. They work with engineering and operations on some aspects of the maintenance and updates of the LDS. Other commonly used names for leak detection support staff are shown in Table E.9.

Table E.9—Other Commonly Used Names for Leak Detection Support Staff

SCADA Support and Network Engineering Staff	SCADA Analyst
SCADA Engineer	Cyber Security Analyst
SCADA System Support Staff	

E.11 Other Stakeholders

There are many stakeholders for leak detection systems. Table E.10 provides categories and commonly used names for these other stakeholders.

Table E.10—Commonly Used Names for Other Stakeholders

Other Support Staff
Commercial and Business Development Personnel
Contract or Operator Emergency Environmental Staff
External Responders
External Emergency Responders
Local Public Safety Officials, First Responders
The Public
General Public
ROW Landowners
Third-party Landowners
Government Agencies or Regulators
PHMSA
State Regulators
NTSB
Connecting Facilities Staff
Employees of other Companies Involved in the Injection or Delivery of the Hazardous Liquids Shipped

E.12 RACI Chart of Leak Detection Stakeholders

An operator may find it useful to develop a RACI chart (see Table 4). The chart lists the key stakeholders and whether they are (R) responsible, (A) accountable, (C) consulted or (I) informed about aspects of the LDP. The training program for those who are accountable or responsible will be at a much higher level than those who are consulted or informed. This RACI chart may not align exactly with the stakeholders' names used in the training sections that follow, because it is an example only (see Annex E for a list of industry roles).

Table E.11—Example RACI Chart of Leak Detection Stakeholders

Responsibilities	Stakeholders							
	Management	Control Center	Analyst	Engineering	IT Group	SCADA Support	Field Operations	Public / Landowners
Aerial Surveillance	A	-	-	-	-	-	R	-
Alarm Management & Threshold	A	R, C, I	I	R	-	R, C, I	I, C	-
Culture / Strategy	R, A	I, C	I	C, I	I	I	I	I
Design	A	I, C	I	R	-	C, I	I	-
Emergency Response	A	R, C, I	-	R	-	I	R	I
Performance	A	I	C	R, C, I	-	R, C, I	-	-
Record Keeping & Reporting	A	R, C, I	-	-	-	-	R	-
Restart Authorization	R, A	C, I	-	I	-	-	C, I	-
Leak / Rupture	R, A	R, C, I	C	C, I	-	-	R, C, I	-
Testing	A	C	C, I	-	-	R	R	-
Training	A	R	I	-	-	R	R	-

Annex F
(informative)

Example Training Program

F.1 General

Table F.1 and subsequent text describe an example of an LDP training program, except for Team Training, which is covered in 11.

Table F.1—Example Roles and Level of Training

	Roles											
Level of Training	**Management**	**Control Center**	**Analyst: Leak Detection Staff**	**Engineering: Support Staff**	**IT Group**	**SCADA Support**	**Field Operations: Field Staff**	**Field Operations: ROW Staff**	**Field Operations: Connecting Facilities Staff**	**Public: External Response**	**Public: Government Agencies or Regulators**	**Public: Land Owners/ROW Users**
LDP Operational	-	X	X	-	-	-	-	-	-	-	-	-
LDP Technical	-	X	X	X	X	X	-	-	-	-	-	-
Internal LD Principles	-	X	X	X	-	X	X	-	-	-	-	-
External LD Principles	-	X	X	X	-		X	X	-	-	-	-
SCADA Deviation Alarms	-	X	X	X	-	X	-	-	-	-	-	-
Pipeline Over/Short Calculations	-	X	X	X	-	-	X	-	-	-	-	-
LDP Awareness	-	X	-	-	-	-	X	X	X	-	-	-
LDP Basics	-	X	-	-	-	-	X	X	-	X	X	X
LDP Regulations/Standards	X	X	X	X	-	-	-	-	-	-	-	-
LDP Strategy & Culture	X	X	X	X	X	X	X	X	-	-	X	-
LDP Management	X	X	X	-	-	-	-	-	-	-	-	-

F.2 Level of Training

F.2.1 General

Each level of training may consist of a set of modules appropriate to the role of the individual. For example, Control Center staff should have a basic understanding of internally based LD technique architecture but do not need the same depth of training on that subject as do leak detection staff. Recommended training content is in the following sections.

F.2.2 LDP Operational Training

LDP operational training is primarily for Controllers and Control Center staff who directly respond to LDP alarms or indicators.

Analysts from the leak detection staff should also understand the operational response to alarms or leak indicators. Content factors are as follows (also see API 1130, Section 6.5, Pipeline Controller Training and Retraining).

— Control Center procedures for leak detection and response. Controller-specific procedures for response to leak detection alarms.

— Hydraulics. Physical principles of hydraulics and concepts of all pipeline operating regimes as they relate to LD techniques, including, for example, the variances of hydraulic pressure due to elevation profiles, batches of differing density (fluid properties), temperature effects, and effects due to DRA, column separation, scrapers, and ILI tools. Controllers should be trained in the basic relationship of pressure and temperature during shut-in conditions. These may include an understanding of pressure tests and hydro tests.

— Alarming/Performance. All LD technique alarming and indicators of LD technique performance. Controllers should be trained in definitions and the proper recognition and response to all LDS alarms. Such alarms include indications of leaks and of the health of the LDS.

— Data Presentation. Recognize of all LDS notifications or alarms and how to research the cause of the alarms (e.g. data failure, irregular operating condition, or possible leak). Other specifics regarding data presentation may be referred to in API 1165.

— Instrument Failure. Impact of an instrument failure on any LDS where the instrument is used.

— Validating LDS Alarms. The operator should undertake an evaluation of the LDS and operating conditions for validating or explaining the cause of an alarm. Controllers should be capable of investigating all alarms, including non-leak alarms, and properly attributing them with assistance from LD staff if needed. Non-leak alarm attribution should be a defined set of causes, for example, data failure, irregular operating condition, or LDS error.

— Line-pack Change. Recognize hydraulic pressure changes due to varying line-pack, including column separation line conditions and their impact on the LDS. A fundamental element in the spectrum of inventory control is the calculation of mass or the comparison of barrels in vs. barrels out. This training would include the ability to recognize the compressibility behavior of the hazardous liquids that are transported.

— Trending. Trending analysis of pipeline variables from SCADA and the LDS.

— LDS Operation. Understand of all LDSs operations and the concept/theory of their operation, including statistical analysis. Interpret alarms correctly and in a timely manner or work with internal or external resources to evaluate the alarm.

— Abnormal Functions. Recognize and react to the abnormal function of an LDS as well as the abnormal function of the SCADA system. Recognize LDS malfunction and degradation due to field equipment or SCADA failure. Understand all failure modes identified through FMEA, RCM analysis, or other techniques and how to recognize and respond to them. For example, if an internally based LDS becomes non-functional or severely degraded due to field equipment or SCADA failure, the Controller should be trained to employ other LDSs or methods to compensate for the loss or degradation of the internally based method.

— Other Leak Detection Techniques. How to employ the results of other LDSs such as reports from field or ROW staff, third-party reports, SCADA deviation alarms, externally based methods, etc., so that an internally based method is not the only means of detecting leaks.

— Basic SCADA / LDS Architecture, Including Networks and Peripheral Devices. Controllers should have a basic understanding of the devices required for the LDS to receive data to function properly including PLCs, switches, routers, network routes, and redundancy of such devices.

— Leak detection staff should understand the limitations of the available LDSs.

F.2.3 LDP Technical Training

LDP technical training is primarily for analysts from the leak detection staff who analyze alarms and maintain internally based LD platforms. Control Center staff should be exposed to this training as well to assist them with initial analysis of alarms. Sections of this training are applicable to Engineering, IT, and SCADA support staff. Content may include:

— details of algorithms and configurations of all LDSs;

— details of computer equipment, including redundancy (architecture and peripherals) of all LDSs;

— details of inhibits, degradation;

— interpretation of in-line inspection (ILI) tool data;

— interpretation of pressure test and hydro test data.

F.2.4 Internally Based LDS Methods Training

Internally based LDS methods training is to familiarize the Control Center staff, analysts, and support staff with the inputs to internally based LDs methods. Content may include:

— basics of internally based LDS method tools and techniques;

— types of equipment used in internally based LDS methods, equipment characteristics, and maintenance effects on internally based LDS methods, including field instrumentation;

— engineering design of internally based LDS methods.

F.2.5 Externally Based LDS Method Training

Externally based LDS method training is for the Control Center staff and analysts who analyze alarms and for engineering support staff and field operations staff tasked with maintaining these LDSs on the pipelines. Content may include:

— types of LDSs installed and how they function;

— visualization of the LDS to the Control Center and locally (leak alarms, leak locations, and health alarms, for example);

— locations;

— sensitivity and interpretation of alarms;

— failure modes;

— operator’s procedures for aerial and ground surveillance and reporting results.

F.2.6 SCADA Deviation Alarm Training

SCADA deviation alarm training is for both Control Center staff and other staff who analyze deviation alarms to understand their significance and the algorithms behind them. Content may include the following.

— typically, a SCADA system-generated event alerts the Controller to an analog data value that has been detected outside a pre-set range.

NOTE These are also called a threshold or range alarms.

— pressure and flow deviation algorithms.

— impact of transients on deviation algorithms and alarms.

— failure modes.

F.2.7 Pipeline Over/Short Training

Pipeline over/short training is for the Control Center staff and analysts who analyze abnormalities and for engineering support and field staff who are tasked with measurement and metering accuracy. Content may include:

— components of over/short calculations and their signage,

— calibrations and uncertainties of instrumentation used,

— adjustment for line pack.

F.2.8 LDP Awareness Training

LDP awareness training is for support staff who do not need LDP technical training but should have an awareness of the various leak indications that are transmitted to the Control Center. The Control Center staff should receive this training so that they know what level of knowledge is expected from field operations staff with whom they interact. Content may include:

— basics of leak detection tools and techniques;

— recognition of a leak and who to call;

— who might call you to report a leak and how to respond;

— aerial appearance of leaks/ruptures and recognition of areas of developing soil instability, landslides, and subsidence;

— sensitive area locations and characteristics.

F.2.9 LDP Basics Training

LDP basics training is primarily for field operations staff and public entities who may observe a leak. The Control Center staff should receive this training so that they know what level of knowledge is expected from field operations staff and public entities with whom they interact. The Control Center staff may work with the existing public awareness program and outreach efforts to ensure that leak detection is covered in those existing programs.

Training content may include:

— pipelines in the area and how to recognize their location,

— damage prevention when using the ROW,

— leak recognition and response,

— public awareness information in API 1162 including,

  — sight, sound, and smell of a leak or the leaked fluid,

  — One Call Centers,

  — National Pipeline Mapping System (NPMS).

F.2.10 LDP Regulations/Standards Training

LDP regulations/standards training are for the Control Center staff, analysts, engineering support, and management who are involved in specifying LDS requirements and reporting incidents.

— Applicable regulations.

— proper completion of form PHMSA F 7000-1, Accident Report—Hazardous Liquid Pipeline Systems.

— state and local regulations on LDPs, surveillance, and release reporting.

— agreements with citizen advisory councils related to LDPs.

— proper data entry to API's PPTS (when used).

— sections that pertain to leak detection in related API documents, including:

  - API 1130,
  - API TR 1149,
  - API 1113,
  - API 1160,
  - API 1161,
  - API 1162,
  - API 1167,
  - API 1168.

— API/AOPL White Paper, Liquid Pipeline Rupture Recognition and Response.

F.2.11 LDP Strategy and Culture Training

LDP strategy and culture training is to provide all staff and regulators with a firm understanding of the framework of the operator's LDP. Content may include:

— a broad overview of the operator's LDP, strategy, and culture;

— how the operator's LDP fits the overall leak detection culture;

— a brief history of significant historical events;

— promotion of safe operations of the pipeline with no negative repercussions on the staff who take actions during leak indications;

— recognition of the hazard of groupthink in leak alarm analysis and promotion of an open exchange of alarm assessments in the Control Room.

F.3.1 LDP Management Training

LDP management training is for the Control Center staff, analysts, and management as the primary personnel responsible for leadership and successful implementation of the operator's LDP. Content may include:

— a detailed overview of the operator's LDP; the structure of this training should follow the outline of this RP for its content.

Emphasis should be placed on:

— operator's strategy and culture;

— overall performance of the LDP, including KPIs and performance targets;

— roles and responsibilities; and

— improvement planning and process.

F.4 Training Methods

F.4.1 General

Table F.2 and subsequent sections describe training roles and training methods.

F.4.2 Classroom

Classroom training should be done through formal, instructor-led, structured classes with verification testing.

Training may include externally based available courses offered by third parties. Testing may be used as a metric to determine effectiveness. This method may be used as a part of initial and refresher training on internally based LDS methods and architecture, externally based LDS methods, over/short analysis, and SCADA deviation alarms.

Table F.2—Example Roles and Methods of Training

	Roles											
Method of Training	**Management**	**Control Center**	**Analyst: Leak Detection Staff**	**Engineering: Support Staff**	**IT Group**	**SCADA Support**	**Field Operations: Field Staff**	**Field Operations: ROW Staff**	**Field Operations: Connecting Facilities Staff**	**Public: External Response**	**Public: Government Agencies or Regulators**	**Public: Land Owners/ROW Users**
Classroom (formal)	X	X	X	X	X	X	X	X	X	-	-	-
Individual Self-Study (informal)	-	X	X	X	X	X	X	-	-	-	-	-
Procedure Review	-	X	X	-	-	-	-	-	-	-	-	-
Interactive Simulation	-	X	-	-	-	-	-	-	-	-	-	-
Playback Simulation	-	X	X	-	-	-	-	-	-	-	-	-
Live Simulation	-	X	X	X	-	X	-	-	-	-	-	-
Real Leak Test	-	X	X	-	-	-	X	-	-	-	-	-
Event Review	X	X	X	-	-	-	X	-	-	-	-	-
On the Job Training	-	X	X	X	X	X	X	X	X	-	-	-
Other: Public Awareness	-	X	-	-	-	-	-	-	-	X	X	X
Other: Site Visit	-	X	-	-	-	-	-	-	X	X	X	-
Team Training (see 13.2.2)	X	X	X	X	-	X	X	X	X	X	X	X

NOTE Some of the training related to leak detection may be covered as a part of Emergency Response Training.

F.4.3 Individual Self-study

Individual self-study may be done through informal, interactive computer-based learning or a short course of reading material with validation testing.

Individual self-study training may be instructor-assisted but does not have the formal syllabus of classroom training.

Testing should be used as a metric to determine effectiveness. This method should be used as a part of refresher training for Control Center and LD staff and may be effective as part of awareness-level training.

F.4.4 Procedure Review

The procedure review should consist of a one-on-one procedure review with stakeholders, inclusive of testing and validation of understanding of procedures and policies related to each individual's role.

F.4.5 Interactive Simulations

The interactive simulations may be computer-based, if available. The operator should validate that the simulator is accurate for leaks.

The more sophisticated a simulator is and the more available it is to the Controller, the better. It may be able to simulate a sampling of representative lines.

F.4.6 Playback Simulations

SCADA playback simulations should show past alarms and behavior during a leak event or non-leak alarm.

Showing the alarms that happened in what sequence with the actual leak or non-leak alarm may help Controllers learn what to look for. The operator's CPM LDP techniques should be pre-configured to capture the data that would be needed to be in alignment with its protocols for conducting a root cause analysis of a real leak.

F.4.7 Live Simulations

For SCADA point analysis, this is primarily accomplished through SCADA data manipulation by modifying pressures, flows or other values used by the alarming logic and by manually overriding them in production to induce an alarm.

These simulations may be announced or unannounced to the Controller. Announced drills typically focus on the LDS alarm and response. Unannounced drills include leak recognition by the Controller as well.

F.4.8 Real Leak Test

The real leak test is like a live simulation, except conducted concurrently with a test of internally based LDS method performance by withdrawing liquid or other means.

For the Control Center staff, the test may be announced or unannounced. If unannounced, this test provides an opportunity to test the Control Center response.

F.4.9 Event Review

Event review and analysis may involve group or individual review of a previous leak event from the operator's history or from investigative documentation from another event in the pipeline industry.

This should focus on lessons learned and similarities and differences between the event and current operations. In addition, this method should include a review of any emergency response procedures that were used in a real event. This review should focus on how closely the procedures were followed and determining their effectiveness. This may provide an opportunity to discuss the team response to a leak or non-leak indication.

F.4.10 On-the-Job Training (OJT)

OJT may involve shadowing of a more experienced individual in the performance of routine and abnormal tasks. This method is appropriate for all roles within the operator's organization.

F.4 Testing/Verification of Training

Validating training effectiveness is achieved through testing and review of testing with the students. The type of test used should be appropriate to the method of delivery. These may be as follows.

— A written examination (knowledge test on paper or electronic format) may be used to evaluate student performance in classroom and individual self-study courses and during site visits.

— Student performance during simulations (interactive, playback, and live), real leak tests, and during on-the-job training may be evaluated like Operator Qualification (OQ) tasks. (Some may actually constitute an OQ task.) An evaluator assesses the student's skills based on a set of predetermined and documented criteria (such as a checklist).

— Event analysis and review, by their nature, are structured and should follow an existing process for abnormal events of all types and may include discussion and documentation of follow-up activity as the validation.

Bibliography

[1] API Recommended Practice 580, *Risk-Based Inspection*

[2] API Recommended Practice 581, *Risk-Based Inspection Technology*

[3] API Recommended Practice 752, *Management of Hazards Associated with Location of Process Plant Permanent Buildings*

[4] API Recommended Practice 753, *Management of Hazards Associated With Location of Process Plant Portable Buildings*

[5] ISO IEC 31010 [2], *Risk management—Risk assessment techniques*

[6] ISO 31000, *Risk management—Principles and guidelines*

[7] US DOT PHMSA ADB-03-04 [3], *Pipeline Industry Implementation of Effective Public Awareness Programs*

[8] US DOT PHMSA ADB-03-08 [4], *Self-Assessment of Pipeline Operator Public Education Programs*

[9] US DOT PHMSA Hazardous Liquid Integrity Management: FAQ [5], Section 9, *Leak Detection, EFRD, and Additional Risk Controls*, FAQs 9.4, 9.5 and 9.6

[10] US DOT [6] PHMSA *Pipeline Safety Stakeholder Communications Fact Sheet: Risk Assessment*

[11] US EPA, EPA-305-D-07-001 [7], *Leak Detection and Repair - A Best Practices Guide,* October 2007

[12] US EPA, EPA-510-S-92-801, *Development of Procedures to Assess the Effectiveness of External Leak Detection Systems*, May 1988

[13] US EPA, EPA-530-UST-90-010, *Standard Test Procedures for Evaluating Leak Detection Systems: Pipeline Leak Detection Systems*, September 1990

[14] US NTSB [8], *Guidance 1 for Strengthening Pipeline Safety Through Rigorous Program Evaluation and Meaningful Metrics*, July 2014.

[15] API 1161, *Recommended Practice for Pipeline Operator Qualification (OQ)*

[16] API Recommended Practice 1165, *Recommended Practice for Pipeline SCADA Displays*

[17] API Recommended Practice 1168, *Pipeline Control Room Management*

[2] International Organization for Standardization, 1, ch ds la Vole-Creuse, CP 56 CH-1211, Geneva 20, Switzerland, www.iso.org.

[3] http://phmsa.dot.gov/pipeline/regs/advisory-bulletin\.

[4] ibid.

[5] http://primis.phmsa.dot.gov/iim/faqa.html.

[6] http://primis.phmsa.dot.gov/comm/FactSheets/FSRiskAssessment.htm.

[7] US Environmental Protection Agency, 1200 Pennsylvania Ave NW, Washington, DC 20460, www.epa.gov.

[8] https://www.federalregister.gov/articles/2014/10/15/2014-24439/pipeline-safety-guidance-for-strengthening-pipeline-safety- through-rigorous-program-evaluation-and.

[18] CSA Z662 [9], *Oil and Gas Pipeline Systems* and Annex E, *Recommended Practice for Liquid Hydrocarbon Pipeline System Leak Detection*

[19] SAE JA1011 [10], *Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes*

[20] OGP11 Report No. 456 [11], *Recommended Practice on Key Performance Indicators*, November 2011

[21] API Recommended Practice 754, *Process Safety Performance Indicators for the Refining and Petrochemical Industries*, 1st Edition

[22] API/AOPL White Paper [12], Liquid Pipeline Rupture Recognition and Response, August 2014

[23] PRCI [13] *Detection of Small Leaks in Liquid Pipelines: Gap Study Analysis of Available Methods*, Catalog No.
L52272

[24] NETL [14] T*echnology Status Report on Natural Gas Leak Detection in Pipelines,* Contract Number: DE-FC26- 03NT41857

[9] Canadian Standards Association, 5060 Spectrum Way, Suite 100, Mississauga, ON J4W 5N6 Canada, www.csa.ca.
[10] SAE International, 400 Commonwealth Drive, Warrendale, PA 15096, www.sae.org.
[11] The International Association of Oil and Gas Producers, 209-215 Blackfriars Road, London Se1 8NL, United Kingdom, www.ogp.org.uk.
[12] Association of Oil Pipelines, 1808 Eye Street NW, Suite 300, Washington, DC 20006, www.aopl.org.
[13] Pipeline Research Council International, 3141 Fairview Park Drive, Suite 525, Falls Church, VA 22042, www.prci.org.
[14] U.S. Department of Energy, National Energy Technology Laboratory, 3610 Collins Ferry Road, P. O. Box 880, Morgantown, WV 26507-0880, www.netl.doe.gov.